

The Joint Money Laundering Steering Group



Prevention of  
money laundering/  
combating terrorist  
financing

2011 review text

GUIDANCE FOR THE UK FINANCIAL SECTOR  
PART III: SPECIALIST GUIDANCE

Amended: December 2011

© Joint Money Laundering Steering Group 2011

Draftsman/Editor: David Swanney

### **PART III: SPECIALIST GUIDANCE**

*This specialist guidance is incomplete on its own. It must be read in the context of the main guidance set out in Part I of the Guidance.*

*This material is issued by JMLSG to assist firms by setting out guidance on how they may approach meeting certain general obligations contained in legislation and regulation, or determining the 'equivalence' of particular overseas jurisdictions or markets, where there is no expectation or requirement in law that such guidance be formally approved by HM Treasury.*

*With the exception of sections 1 and 5, therefore, the guidance in this Part does not carry the same Ministerial approval as the guidance in Parts I and II.*

#### **CONTENTS**

- 1.\* Transparency in electronic payments (Wire transfers)**
- 2. Equivalent jurisdictions**
- 3. Equivalent markets**
- 4. Compliance with the UK financial sanctions regime**
- 5.\* Directions under the Counter-Terrorism Act 2008, Schedule 7**

\*These sections carry HM Treasury Ministerial approval



## 1: Transparency in electronic payments (Wire transfers)

*Note: This section may only be relevant to a limited number of firms in the financial sector (see Part I, paragraphs 5.2.10ff). It previously formed the 'Wire Transfers' guidance in Part II and has now been moved to Part III and extended to include cover payments. Part A refers to FATF SR VII and Part B to Cover Payments.*

### PART A – FATF SRVII

#### Background

- 1.1 FATF issued Special Recommendation VII in October 2001, with the objective of enhancing the transparency of electronic payment transfers (“wire transfers”) of all types, domestic and cross border, thereby making it easier for law enforcement to track funds transferred electronically by terrorists and criminals. A revised Interpretative Note to this Special Recommendation was issued by the FATF on 10 June 2005, further revised on 29 February 2008, and is available at <http://www.fatf-gafi.org/dataoecd/34/56/35002635.pdf>
- 1.2 Special Recommendation VII is addressed to FATF member countries, and was implemented in member states of the European Union, including the UK, through Regulation 1781/2006, which is at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:345:0001:0009:EN:PDF>
- 1.3 The Regulation requires the ordering financial institution to ensure that all wire transfers carry specified information about the originator (Payer) who gives the instruction for the payment to be made. The core requirement is that this information consists of name, address and account number; however, there are a number of permitted variations and concessions, see below under **Information Requirements** (paragraphs 1.13ff).
- 1.4 As the text of this Regulation has EEA relevance, the three non-EU Member States of the EEA, i.e., Iceland, Liechtenstein and Norway, are expected to enact equivalent legislation. As and when this happens, references in this guidance to *intra-EU* can be understood to include these states. However, for the time being the reduced information requirement available within the EU will not apply to payments to and from those countries.
- 1.5 During 2008, the AML Task Force of the three Level 3 Committees (European Banking Supervisors, Securities Regulators and Insurance and Operational Pensions) investigated the varying approaches of Payment Service Providers across the EU to the inward monitoring obligations contained in the Regulation. Following consultation with industry and others, they published in October 2008 a ‘Common Understanding’ designed to achieve a more consistent approach by Payment Service Providers. Further details are set out at paragraphs 1.30 and Annex 1-II.

#### Scope of the Regulation

- 1.6 The Regulation is widely drawn and intended to cover all types of funds transfer falling within its definition as made “by electronic means”, other than those specifically exempted wholly or partially by the Regulation. For UK-based Payment Service Providers (PSPs) it therefore includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various Euro

payment systems, and domestic transfers via CHAPS and BACS. The Regulation specifically exempts the following payment types:

- transfers where both Payer and Payee are PSPs acting on their own behalf - this will apply to MT 200\* series payments via SWIFT. This exemption will include MT 400 and MT 700 series messages when they are used to settle trade finance obligations between banks (\*cover payments using MT 202/205COVs are, however, in scope – see Part B of this guidance);
- transfers by credit or debit card or similar payment instrument, providing that the Payee has an agreement with the PSP permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the Payer (see paragraph 1.17);
- transfers whereby the Payer withdraws cash from his/her own account. This is designed to exempt ATM withdrawals outside the EU which would otherwise attract the full information requirement;
- transfers to public authorities for taxes, fines or other levies;
- direct debits, subject to their carrying a unique identifier for tracing purposes;
- truncated cheques (cheques are otherwise paper to which the Regulation does not apply);
- Article 3 (4) provides a limited exemption for small pre-paid transfers carried out by means of a mobile phone or any other digital or IT device;
- e-money transfers, as defined in Article 11(5)(d) of the Third EU Money Laundering Directive, where they do not exceed €1000. i.e., those transfers transacted using non-reloadable electronic money products on which the maximum load does not exceed € 150, or using reloadable e-money products which are subject to a maximum load of €2500 in a calendar year and maximum redemption of under €1000 in the same calendar year. (see also Part II Sector 3: *Electronic money*);
- post-paid funds transfers carried out by mobile phone, or any other digital or IT device, subject to various conditions, including their traceability and that they relate to the provision of goods and services.

1.7 The following payment types are also exempt under the Regulation (under derogations which are not used in the UK):

- Article 3 (6), which exempts small payments for goods and services, relates to giro payment systems in a few other member states;
- funds transfers of €150 or less for charitable, religious, cultural, educational, social, scientific or fraternal purposes to a prescribed group of non-profit organisations which run annual / disaster relief appeals and which are subject to reporting and external audit requirements or supervision by a public authority and whose names and supporting details have been specifically communicated by the Member State to the Commission. This applies only to transfers within the territory of the Member State. The exemption is designed to ensure that small charitable donations to certain bona fide bodies are not frustrated, but has limited practical relevance in the

UK, where typical mechanisms for making payments to charities, e.g., by credit transfer or by card payment within the EU, will either not be subject to the Regulation, or where they are, will be compliant with it in any case;

- 1.8 The UK credit clearing system is out of scope of the Regulation as it is paper-based and hence transfers are not carried out “by electronic means”. Cash and cheque deposits over the counter via bank giro credits are not therefore affected by the Regulation.

Note: The Regulation defines “Payee” as a natural or legal person who is the intended final recipient of transferred funds. Recognizing that a perverse and wholly unworkable interpretation could be put on those words, where a named Payee might have been a conduit for an undisclosed ‘final recipient’ to serve a criminal objective, this Guidance takes the position that ‘final recipient’ can only practically be understood as referring to the party named in the transfer as the beneficiary of the payment.

See paragraph 1.18 below in relation to the merchant acquisition payment process.

### **Pre-conditions for making payments**

- 1.9 Payment Service Providers (PSPs) of Payers must ensure that the Payer information conveyed in the payment relating to account holding customers is accurate and has been verified. The verification requirement is deemed to be met for account holding customers of the PSP whose identity has been verified, and where the information obtained by this verification has been stored in accordance with anti money laundering requirements, ie in the UK in accordance with the Money Laundering Regulations 2007, which gave effect to the Third EU Money Laundering Directive. This position applies even though the address shown on the payment transfer may not have been specifically verified. No further verification of such account holders is required, although PSPs may wish to exercise discretion to do so in individual cases; e.g., firms will be mindful of Part I, paragraphs 5.3.14 – 5.3.18, concerning customers with existing relationships. (See 1.13ff where the named Payer is not the holder of the account to be debited.)
- 1.10 Before undertaking one-off payments in excess of €1000 on the instructions of non-account holding customers, the PSP of the Payer should verify the identity and address (or evidence of a permitted alternative to address, such as date and place of birth if quoting that information on the transfer instead of address).
- 1.11 For non-account based transfers of €1000 and under, PSPs are not required by the Regulation to verify the Payer’s identity except when several transactions are carried out which appear to be linked (see Article 5.4) and together exceed €1000. NB, even in cases where the Regulation does not require verification, the customer information has to be obtained and it may be advisable for the PSP to verify the identity of the Payer in all cases.
- 1.12 Evidence of verification must be retained with the customer information in accordance with **Record Keeping Requirements** (see 1.20-1.21).

### **Information Requirements**

#### **1.13 Complete payer information:**

Except as permitted below, complete Payer information must accompany all wire transfers. Effectively, the complete Payer information requirement applies where the destination PSP is located in a jurisdiction outside the European Union. Complete Payer information consists of: name, address and account number.

- Address ONLY may be substituted with the Payer's date and place of birth, or national identity number or customer identification number. This Guidance recommends that these options are only deployed selectively within a firm's processes to address particular needs. It follows that in the event a Payee PSP demands the Payer's address, where one of the alternatives had initially been provided, the response to the enquiry should point that out. Only with the Payer's consent or under judicial compulsion should the address be additionally provided.
- Where the payment is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier which permits the payment to be traced back to the Payer.
- The extent of the information supplied in each field will be subject to the conventions of the messaging system in question and is not prescribed in detail in the Regulation.
- The account number could be, but is not required to be, expressed as the IBAN (International Bank Account Number).
- The Regulation applies even where the Payer and Payee hold accounts with the same PSP.
- Where a bank is itself the Payer, as will sometimes be the case even for SWIFT MT 102 and 103 messages, this Guidance considers that supplying the Bank Identifier Code (BIC) constitutes complete Payer information for the purposes of the Regulation, although it is also preferable for the account number to be included where available. The same applies to Business Entity Identifiers (BEIs), although in that case the account number should always be included. As the use of BICs and BEIs is not specified in FATF Special Recommendation VII or the Regulation, there may be requests from Payee PSPs for address information.
- Generally, firms will populate the information fields from their customer database. In cases where electronic banking customers input their details directly the Payer's PSP is not required, at the time that the account is debited, to validate the Payer's name and/or address against the name and address of the accountholder whose account number is stated on the payment transfer.
- Where the named Payer is not the accountholder the Payer's PSP may either substitute the name and address (or permitted alternatives) of the account holder being debited (subject to any appropriate customer agreement), or execute the payment instruction with the alternative Payer name and address information provided with the consent of the accountholder. In the latter case, provided the Payer PSP retains all relevant data for 5 years, the Payer PSP is required to verify only the information about the accountholder being debited (in accordance with Article 5.3a. of the Regulation). PSPs should exercise a degree of control to avoid abuse of the discretion by customers.

It is important to note that this flexibility should not undermine the transparency of Payer information sought by FATF Special Recommendation VII and the Regulation. It is designed to meet the practical needs of corporate and other business (e.g., solicitor)

accountholders with direct access who, for internal accounting reasons, may have legitimate reasons for quoting alternative Payer details with their account number.

- Where payment instructions are received manually, for example, over the counter, the Payer name and address (or permitted alternative) should correspond to the account holder. Any request to override customer information on a similar basis to that set out above for electronic banking customers should be contained within a rigorous referral and approval mechanism to ensure that only in cases where the PSP is entirely satisfied that the reason is legitimate should the instruction be exceptionally dealt with on that basis. Any suspicion arising from a customer's behaviour in this context should be reported to the firm's Nominated Officer.
- Beneficiary information: whilst Regulation 1781/2006 is concerned only with information relating to the Payer it is also important that Payer PSPs include sufficient beneficiary information to mitigate the risks of customer funds being incorrectly blocked, delayed or rejected.
- Payee PSPs are not obligated to pass on to the payee all the payer information they receive with a transfer. However, paragraph 38 of the Payment Services Regulations provides inter alia that:

"The payee's payment service provider must, immediately after the execution of the payment transaction, provide or make available to the payee the information specified in paragraph (2).

(2) The information referred to in paragraph (1) is—

(a) a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;"

#### 1.14 Reduced Payer Information:

Where the PSPs of both Payer and Payee are located within the European Union, wire transfers need be accompanied only by the Payer's account number or by a unique identifier which permits the transaction to be traced back to the Payer.

- However, if requested by the Payee's PSP, complete information must be provided by the Payer's PSP within three working days, starting the day after the request is received by the Payer's PSP. ("Working days" is as defined in the Member State of the Payer's PSP).
- Article 17 of the Regulation provides for the circumstances in which transfers of funds between EU Member States and territories outside the EU with whom they share a monetary union and payment and settlement systems may be treated as transfers within the Member State, so that the reduced information requirement can apply to payments passing between that Member State and its associated territory (but not between any other Member State and that territory). In the case of the UK such arrangements will include the Channel Islands and the Isle of Man.
- Firms which avail themselves of the option to provide reduced payer information in intra-EU transfers should bear in mind that they may face requests for additional information (especially name) from payee banks for the purpose of sanctions screening (see section 4: *Compliance with the UK financial sanctions regime*, paragraph [4.61]).

### 1.15 Batch File Transfers:

A hybrid complete/reduced requirement applies to batch file transfers from a single Payer to multiple Payees outside the EU in that the individual transfers within the batch need carry only the Payer's account number or a unique identifier, provided that the batch file itself contains complete Payer information.

### 1.16 Payments via Intermediaries:

Intermediary PSPs (IPSPs) must, subject to the following guidance on technical limitations, ensure that all information received on the Payer which accompanies a wire transfer is retained with the transfer.

It is preferable for an IPSP to forward payments through a system which is capable of carrying all the information received with the transfer. However, where an IPSP within the EU is technically unable to on-transmit Payer information originating outside the EU, it may nevertheless use a system with technical limitations provided that:

- if it is aware that the Payer information is missing or incomplete it must concurrently advise the Payee's PSP of the fact by an agreed form of communication, whether within a payment or messaging system or otherwise.
- it retains records of any information received for five years, whether or not the information is complete. If requested to do so by the Payee's PSP, the IPSP must provide the Payer information within three working days of receiving the request.

### 1.17 Card transactions

As indicated in paragraph 1.6, card transactions for *goods and services* are out of scope of the Regulation provided that a unique identifier, allowing the transaction to be traced back to the payer, accompanies the movement of the funds. The 16 digit Card PAN number serves this function.

Similarly, the Card PAN number meets the information requirement for all Card transactions for any purpose where the derogation for transfers within the European Union applies, as explained in and subject to the conditions set out in paragraph 1.14.

Complete payer information is required in all cases where the card is used to generate a direct credit transfer, including a balance transfer, to a payee whose PSP is located outside the EU. These are "push" payments, and as such capable of carrying the information when required under the Regulation.

Otherwise, Card transactions are "pull" payments, i.e., the transfer of funds required to give effect to the transaction is initiated by the merchant recipient rather than the Card Issuer and under current systems it is not possible for any information in addition to the PAN number to flow with the transfer in those cases where the transaction is arguably not for 'goods and services' but is settled to a PSP outside the EU. Examples include Card transactions used to make donations to charity, place bets, or purchase e-money products such as prepaid cards. As a matter of expediency these transactions must therefore be treated as 'goods and services'. FSA and HM Treasury have supported that interpretation for the time being, subject to further review at an unspecified future date on the basis that the transactions are traceable by the PAN number.

### 1.18 Merchant Acquisition

Part II sector 2: *Credit cards* paragraphs 2.9-2.11 briefly describe the payment processing service provided by merchant acquirers in respect of debit and credit card transactions undertaken at point of sale terminals or on the internet. For internet-based transactions a separate PSP, operating under a contractual agreement with the merchant in the same way as a merchant acquirer, may act as a payment gateway to the payment clearing process interfacing as necessary with the merchant's acquirer. These internet PSPs may also accommodate payment methods in addition to cards.

A more detailed explanation of the processing of card transactions may be found in Annex 5 of the FSA's October 2009 Approach document in relation to the Payment Services Regulations. <http://www.fsa.gov.uk/Pages/About/What/International/psd/>

There are two distinct funds transfers within the overall payment process: first, the collection by the merchant acquirer via the card schemes of the cardholder's funds from the card issuing firm where he holds his account (or where other payment methods are used the funds are collected by the internet PSP direct from the purchaser); secondly, the merchant acquirer (or the internet PSP for non-card transactions) pays the funds over in a separate transaction to the merchant's bank account. The second transfer will normally be a consolidated settlement payment following reconciliation, which aggregates many different transactions, and is made net of fees after an agreed period of time to safeguard against transaction disputes. Details of the underlying transactions are made available to the merchant for its own reconciliation purposes.

Consequently, for the purposes of the Regulation, the internet PSP or merchant acquirer is not an intermediary PSP but is rather the PSP of the payee and is subject to the obligations described in chapter 3 of the Regulation to the extent that they are relevant, i.e., in relation to electronic funds transfers other than card transactions which enjoy a qualified exemption under Article 3(2) of the Regulation. So far as the merchant's bank is concerned the merchant acquirer or the internet PSP is the 'Payer' of the separate consolidated settlement payment and that bank does not receive or require the underlying cardholder PAN number information (or payer details for non-card transactions).

Although the payment process operates in the way described, it should be noted that a full audit trail is available in case of need so that the traceability objective of the Regulation is in no way compromised.

### 1.19 Minimum standards

The above information requirements are minimum standards. It is open to PSPs to elect to supply complete Payer information with transfers which are eligible for a reduced information requirement and thereby limit the likely incidence of inbound requests for complete information. (In practice a number of large UK and European banks have indicated that they will be providing complete payer information for all transfers where systems permit). To ensure that the data protection position is beyond any doubt, it would be advisable to ensure that terms and conditions of business include reference to the information being provided.

### Record Keeping Requirements

- 1.20 The Payee's PSP and any intermediary PSP must retain records of any information received on a Payer for five years, in accordance with the Regulation.

- 1.21 The Payer's PSP must retain records of transactions and supporting evidence of the Payer's identity in accordance with Part I, Chapter 8.

### Checking Incoming Payments

- 1.22 Payee PSPs should have effective procedures for checking that incoming wire transfers are compliant with the relevant information requirement. In order not to disrupt straight-through processing, it is not expected that monitoring should be undertaken at the time of processing the transfer. The Regulation specifies that PSPs should have procedures to detect whether relevant information is missing. (It is our understanding that this requirement is satisfied by the validation rules of whichever messaging or payment system is being utilised). Additionally, the Regulation requires PSPs to take remedial action when they become aware that an incoming payment is not compliant. Hence, in practical terms it is expected that this requirement will be met by a combination of the following:

- (i) SWIFT payments on which mandatory Payer information fields are not completed will fail anyway and the payment will not be received by the Payee PSP. Current SWIFT validation prevents payments being received where the mandatory information is not present at all. However, it is accepted that where the Payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system. Similar considerations apply to non-SWIFT messaging systems which also validate that a field is populated in accordance with the standards applicable to that system, e.g., BACS.
- (ii) SWIFT has reviewed how its validation standards might be improved to facilitate inward monitoring, as a result of which Option F has been introduced as one of the three available formatting options. Option F structures information systematically by means of specified identifier codes and formatting conventions. However, use of this Option is not mandatory.
- (iii) PSPs should therefore subject incoming payment traffic to an appropriate level of post event random sampling to detect non-compliant payments. This sampling should be risk based, e.g.:
  - the sampling could normally be restricted to payments emanating from PSPs outside the EU where the complete information requirement applies;
  - the sampling could be weighted towards non FATF member jurisdictions, particularly those deemed high risk under a PSP's own country risk assessment, or by reference to external sources such as Transparency International, or FATF or IMF country reviews);
  - focused more heavily on transfers from those Payer PSPs who are identified by such sampling as having previously failed to comply with the relevant information requirement;
  - Other specific measures might be considered, e.g., checking, at the point of payment delivery, that Payer information is compliant and meaningful on all transfers that are collected in cash by Payees on a "Pay on application and identification" basis.

NB. Whenever these measures reveal potentially suspicious transactions, the normal reporting obligations apply (see Part I, Chapter 6).

- 1.23 If a Payee PSP becomes aware in the course of processing a payment that it contains meaningless or incomplete information, under the terms of Article 9 (1) of the Regulation it should either reject the transfer or ask for complete information on the Payer. In addition, in such cases, the Payee PSP is required to take any necessary action to comply with any applicable law or administrative provisions relating to money laundering and terrorist financing. Dependent on the circumstances such action could include making the payment or holding the funds and advising the Payee PSP's Nominated Officer.
- 1.24 Where the Payee PSP becomes aware subsequent to processing the payment that it contains meaningless or incomplete information either as a result of random checking or other monitoring mechanisms under the PSP's risk-based approach, it must:
- (i) seek the necessary information on the Payer
- and/or
- (ii) take any necessary action under any applicable law, regulation or administrative provisions relating to money laundering or terrorist financing.
- 1.25 PSPs will be mindful of the risk of incurring civil claims for breach of contract and possible liability if competing requirements arise under national legislation, including in the UK the Proceeds of Crime Act and other anti money laundering and anti terrorism legislation.
- 1.26 Where a PSP is identified as having regularly failed to comply with the information requirements, under Article 9(2) the Payee PSP should take steps, which may initially include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that PSP or deciding whether to terminate its relationship with that PSP either completely or in respect of funds transfers.
- 1.27 Under Article 10 a Payee PSP should consider whether incomplete or meaningless information of which it becomes aware on a funds transfer constitutes grounds for suspicion which would be reportable to its Nominated Officer for possible disclosure to the Authorities.
- 1.28 With regard to transfers from PSPs located in countries that are not members of either the EU or FATF, firms should endeavour to transact only with those PSPs with whom they have a relationship that has been subject to a satisfactory risk-based assessment of their anti money laundering policies and procedures and who accept the standards set out in the Interpretative Note to FATF Special Recommendation VII.
- 1.29 It should be borne in mind when querying incomplete payments that some FATF member countries outside the EU may have framed their own regulations to incorporate a threshold of €/US\$ 1000 below which the provision of complete information on outgoing payments is not required. This is permitted by the Interpretative Note to FATF Special Recommendation VII. The USA is a case in point. This does not preclude European PSPs from calling for the complete information where it has not been provided, but it is reasonable for a risk-based view to be taken on whether or how far to press the point.
- 1.30 As indicated in paragraph 1.5, the inward monitoring requirements of the Regulation were elaborated on in the *Common Understanding* (CU) published in October 2008 by the AML Task Force of three European regulatory bodies. The CU positioned itself as a "clarification" of the Regulation's requirements, not an "extension" of them. Whilst the final document was less

prescriptive than the Task Force's starting position the expectations set out are fairly detailed, covering the various elements within the Regulation, viz

- Sampling and filtering of incoming payments
- Deadlines for remediating deficient transfers
- Identifying regularly failing Payment Service Providers

all of which should be enshrined by firms within a clearly articulated set of policy and processes approved at an appropriately senior level defining the approach to be adopted to discharge these requirements Annex 1-II sets out a broad summary of the requirements, but firms should refer directly to the CU for the detail. See:

<http://www.c-eps.org/getdoc/d399f8d4-c2e4-4cce-8141-1aff447bb189/The-three-Level-3-Committees-publish-today-their-c.aspx>

## PART B – COVER PAYMENTS

### Background

- 1.31 A customer funds transfer usually involves the ordering customer (originator) instructing its bank (the originator's bank) to make a payment to the account of a payee (the beneficiary) with the beneficiary's bank. In the context of international funds transfers in third party currencies, the originator's bank will not usually maintain an account with the beneficiary bank in the currency of the payment that enables them to settle the payment directly. Typically, intermediary (or covering) bank(s) are used for this purpose, usually (but not always) located in the country where the currency of the payment is the national currency. The alternative but less efficient method of making such payments is by serial MT103.
- 1.32 Cover payments are usually effected via SWIFT and involve two distinct message streams:
- A customer payment order (usually a SWIFT Message Type (MT)103) which is sent by the originator's bank direct to the beneficiary's bank and carries payment details, including originator and beneficiary information;
  - A covering bank-to-bank transfer (the cover payment - historically, a SWIFT MT202) which is sent by the originator's bank to an intermediary bank (usually its own correspondent) asking the intermediary bank to 'cover' the originator bank's obligation to pay the beneficiary bank. The intermediary bank debits the originator bank's account and either credits the beneficiary bank's account under advice, or if no account is held, sends the funds to the beneficiary bank's correspondent with settlement usually being effected through the local Real Time Gross Settlement System (RTGS). The beneficiary bank is then able to reconcile the funds that it receives on its correspondent account with the MT103 received direct from the originator's bank.
- 1.33 Payments are sent using the 'cover method' primarily to avoid delays associated with differing time zones and to reduce the costs associated with commercial transactions.

### Transparency Issues:

- 1.34 Historically, the MT202 has been used either to effect cover for an underlying customer transfer (MT103) or for inter-bank payments that are unconnected to customer transfers, such as wholesale money market or foreign exchange transactions. Consequently, an intermediary bank would not necessarily know that it was dealing with a cover payment when processing an MT202 message. Additionally, as there is no provision within the MT202 message format for it to carry the originator and beneficiary information that is contained in an underlying MT103 customer transfer, an intermediary bank has not, hitherto, been in a position to screen or monitor underlying customer information in relation to cover payments, from a sanctions or ML/FT perspective.
- 1.35 To improve transparency in respect of cover payments, and in order to assist financial institutions with their sanctions and AML/CFT obligations, SWIFT created a variant of the MT202, being the MT202COV<sup>1</sup>, which has, since the 21<sup>st</sup> November 2009 go-live date, enabled originator and beneficiary information contained in the MT103 customer transfer to be replicated in certain fields of the MT202COV (further details can be found at [www.swift.com](http://www.swift.com)):

<sup>1</sup> For cover payments effected between originator and beneficiary banks located in the same jurisdiction using a third party currency, an MT205COV can be used instead of an MT202COV and references in this guidance to MT202COV also relate to MT205COV.

- 1.36 The MT 202COV should be used for all outgoing cover payment transactions for which there is an associated MT103 and must replicate the originator/beneficiary information contained in the MT 103. The existing MT 202 should in future be used only for bank to bank transactions. As soon as technically feasible after the 21<sup>st</sup> November 2009 go-live date, firms should have the capability to receive MT202COV messages from other banks and, as a minimum, screen them against mandatory lists of individuals and entities whose assets must be blocked, rejected or frozen.
- 1.37 As an alternative to sending customer payments using the 'cover method', banks can choose to send their payments by the 'serial method' in which an MT103 is sent by the originator's bank to its correspondent asking for payment (and the corresponding covering funds) to be made available to the beneficiary bank for account of the beneficiary.

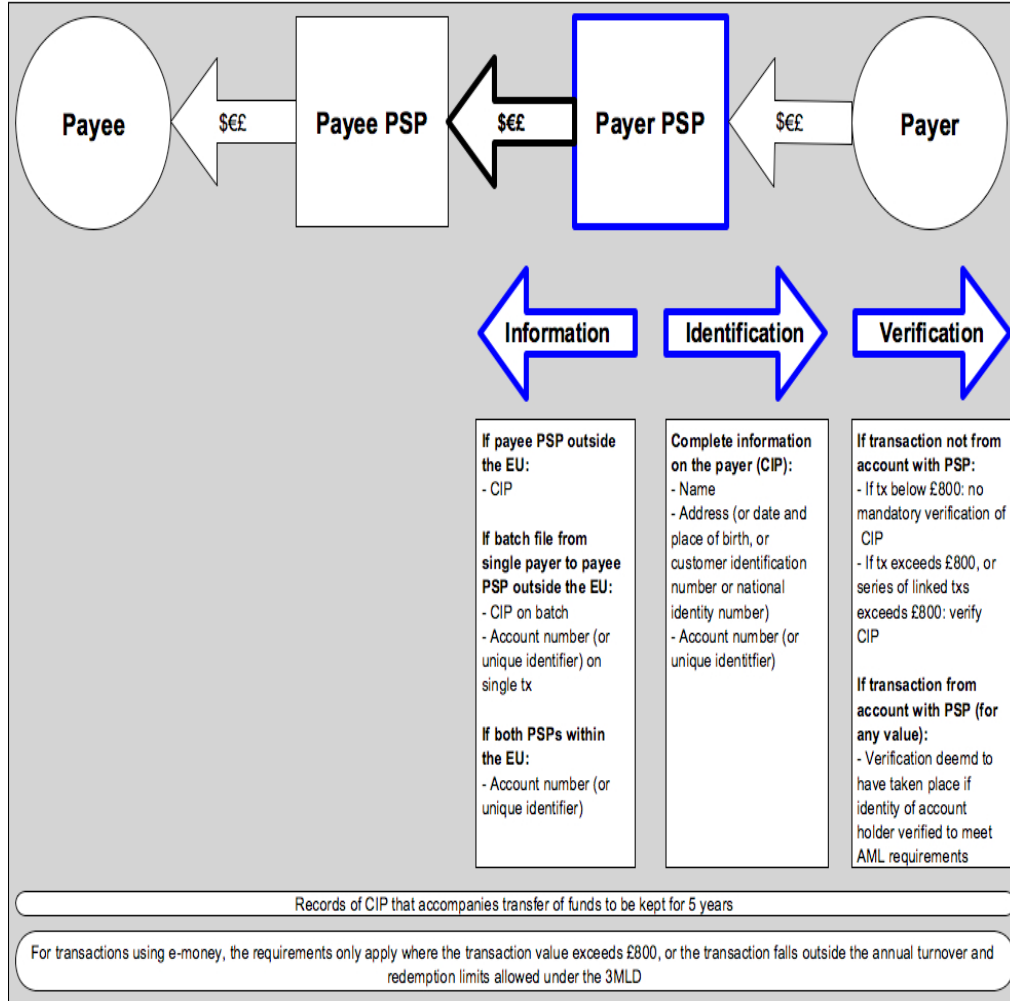
#### **Further Guidance**

- 1.38 After consulting with industry and regulators, in May 2009 the Basel Committee on Banking Supervision (BCBS) issued a paper entitled 'Due diligence and transparency regarding cover payment messages related to cross-border wire transfers', which is available at [www.bis.org](http://www.bis.org) and provides further guidance for banks processing cover payments. This guidance is not mandatory and currently has no formal legal or regulatory force in the UK.,

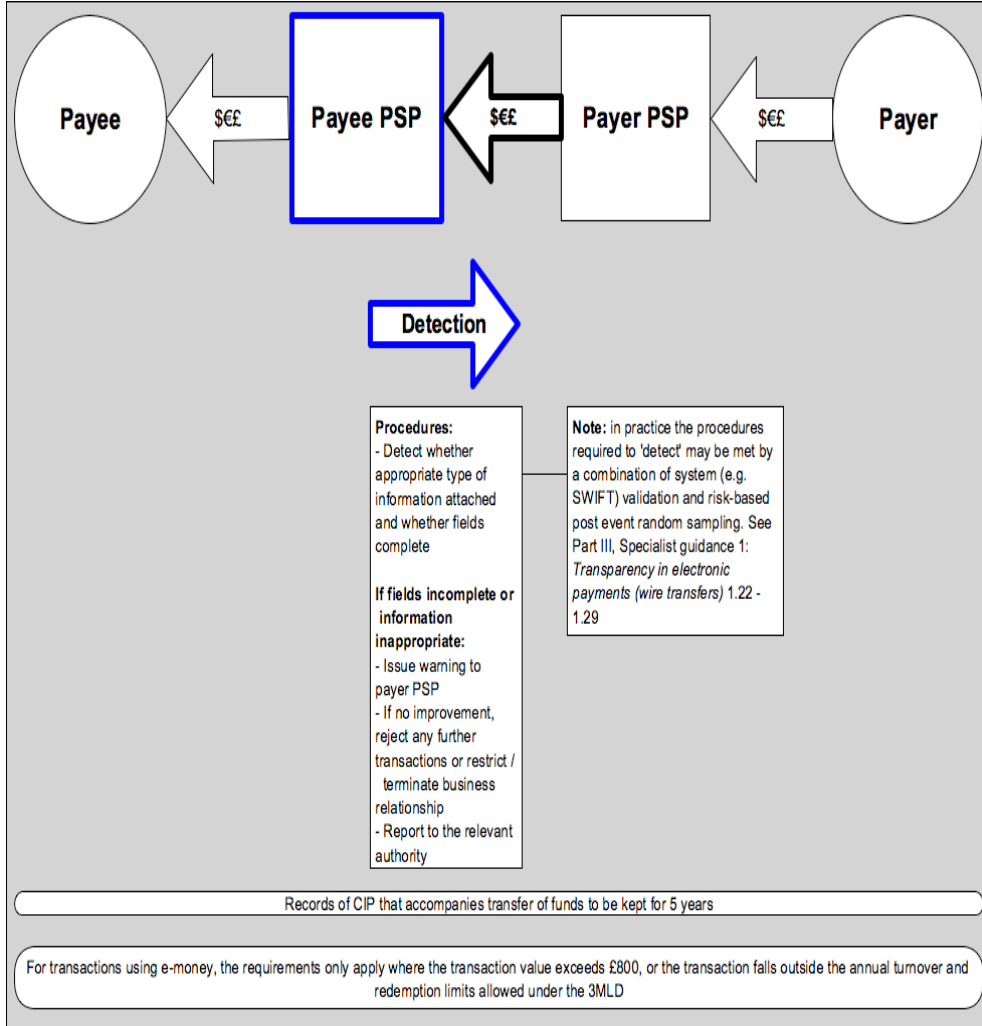
#### **Other Useful Sources of Information:**

1. SWIFT Press release. 'New Standards for Cover Payments' (May 19 2009), available at <http://www.swift.com/>.
2. 'Guidelines for use of the MT202COV' issued by the Payments Market Practice Group, available at <http://pmpg.webex.one.com/default.asp?link>
3. 'Cover Payments: Background Information and implications of the new SWIFT Message Format' and 'The Introduction of the MT202COV in the International Payment Systems,' issued jointly in May 2009 by the Bankers' Association for Finance and Trade, the Clearing House Association LLC, the European Banking Federation, the International Banking Federation, the International Chamber of Commerce, the International Council of Securities Associations, the International Financial Services Association, SWIFT and the Wolfsberg Group, available at the respective web sites of these organisations.

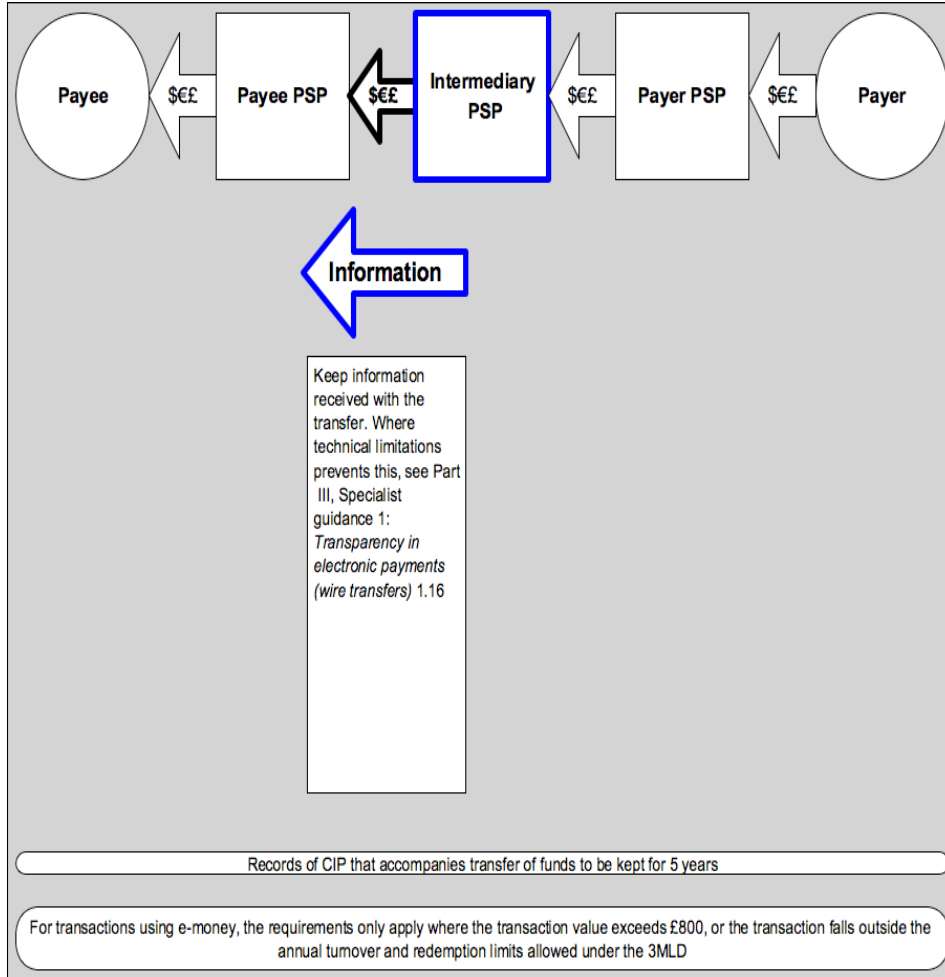
**Scenario 1: Transfer of funds – Obligations on Payer PSP**



**Scenario 2: Transfer of funds – Obligations on Payee PSP**



**Scenario 3: Transfer of funds – Obligations on Intermediary PSP**



## Summary of the ‘Common Understanding’

For background, refer to paragraphs 1.5 and 1.30.

The following is a summary only – firms should refer directly to the Common Understanding for the detail. See: <http://www.c-eps.org/getdoc/d399f8d4-c2e4-4cce-8141-1aff447bb189/The-three-Level-3-Committees-publish-today-their-c.aspx>

### 1. Sampling / Filtering:

The CU accepted the basic premise of system validation as the first line of defence, which in the absence currently of a standard filter will inevitably allow some deficient payments to be accepted. Hence, PSPs should deploy two types of control

- **post event sampling:** unless PSPs can detect incomplete or meaningless payments at the time of processing a transfer the CU supports the position that there should be risk based, post event sampling to detect non compliant payments. To fulfil the risk based criterion, sampling could focus on transfers from higher risk sending PSPs, especially those previously identified as having failed to comply with the relevant information requirements.
- **filtering for ‘obvious meaningless information’** defined as ‘information clearly intended to circumvent the intention of the Regulation’: this is not a mandatory control, rather PSPs are ‘encouraged’ to apply such filters. What is in mind here are formulations such as ‘one of our customers’ or any form of words which on the face of it is not providing genuine sender information.
- PSPs are expected to take action on all incomplete or meaningless transfers that they become aware of. Depending on whether they become aware at the time of processing or subsequently they should take action on all such defective transfers so identified in the form of one of the three response options: (1) reject the transfer, (2) hold it and ask for missing information, (3) process the payment and ask for missing information.
- Subject to any overriding legal restraints in their own jurisdiction PSPs are urged not to rely only on the No 3 post event follow-up option but to deploy the other options when appropriate. (N.B. The BBA took the position in their response to the consultation that other than in exceptional circumstances rejection of payment or delay in processing was quite unacceptable from a customer service perspective).

### 2. Deadlines for remediating deficient transfers:

When requesting missing information PSPs should work to appropriate and self imposed deadlines. The CU suggested what it considered to be reasonable timeframes for this purpose. In the absence of a satisfactory response the sending PSP should be warned that it may in future be subject to high risk monitoring (under which all or most of its future payments would be subject to scrutiny). Consideration should also be given as to whether the deficient payment is ‘suspicious’ and should be reported.

### 3. Identifying regularly failing PSPs

Mutual policing of PSPs is intended to go beyond the remediation of individual deficient payments to a systematic assessment of those PSPs who persistently fail to provide the information required under the Regulation. A receiving PSPs is therefore expected to establish criteria for determining when a PSP who is sending payments is 'regularly failing' such that some form of disciplinary reaction is called for. Five examples are given of the criteria that might be adopted for this sort of data analysis. Thereafter it is expected firstly to notify the failing PSP that it has been so identified in accordance with the common understanding. Secondly, it must notify its regulator of the identity of the failing PSP. The CU acknowledges that whilst the Regulation states that a receiving PSP should decide whether in these circumstances to restrict or terminate its business relationship with a failing PSP, in practice such decisions must weigh up other factors and business considerations – implicitly it accepts that hasty action is not appropriate and should so far as possible be consensual with peer PSPs and have the benefit of supervisors' input before draconian disciplinary action is taken.

#### **4. Articulation of internal policy, processes and procedures**

A PSP is expected to have in place a clearly articulated policy approved at an appropriately senior level defining the approach to be adopted to discharge the obligations outlined under 1-3 above, e.g., covering inter alia.

- when to reject, execute and query, hold and query
- its risk criteria
- how soon after receipt of transfer it will raise the query (i.e., if batching up queries the CU recommends it should be no more than seven days)
- the deadlines it will impose for responses and further follow up
- how it will assess whether incomplete or meaningless transfers are 'suspicious'
- the criteria it will apply based on the guidelines in paragraph 43 to identify 'regularly failing' payer PSPs, who must then be notified as such and reported to the relevant authority.

## 2: Equivalent jurisdictions

*This guidance is issued to assist firms by setting out how they might approach their assessment of other jurisdictions, to determine whether they are 'equivalent'. Although it is not formal guidance that has been given Ministerial approval, it has been discussed with HM Treasury and reflects their input.*

*The guidance discusses jurisdictions where there may be a presumption of equivalence, and those where such a presumption may not be appropriate without further investigation. It then discusses issues that a firm should consider in all cases when coming to a judgement on whether a particular jurisdiction is, in its view, equivalent.*

### 2.1 What is an "equivalent jurisdiction" and why does it matter?

The 3rd European Council Directive on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the money laundering directive), whilst setting out (in articles 6-9) the obligation on firms to carry out specific customer due diligence (CDD) measures, allows firms (article 11) to carry out simplified due diligence (SDD) in respect of other firms which are subject to the provisions of the directive, and to rely (article 16) on other firms that are subject to the provisions of the directive to carry out CDD measures on their behalf. The money laundering directive also extends these derogations to firms in third countries, in those jurisdictions where they are subject to legal obligations that are 'equivalent' to those laid down in the directive, and where they are supervised for compliance with those obligations.

The Money Laundering Regulations 2007 (the 2007 Regulations) implement the provisions of the money laundering directive into UK law. The 2007 Regulations provide (Regulation 13) that firms may apply SDD where the customer is itself a credit or financial institution which is subject to the requirements of the money laundering directive, or is situated in a non-EEA state which imposes requirements equivalent to those laid down in the money laundering directive. The Regulations also permit (Regulation 17) reliance on firms which carry on business in a non-EEA state which is subject to requirements equivalent to those laid down in the money laundering directive, and which are supervised for compliance with those requirements, to carry out CDD on the relying firm's behalf.

It should be noted that the basis for the exemption in the directive and the Regulations is focused on the provisions of the legislation in a particular jurisdiction, rather than what actually happens in practice (although firms have to be supervised for compliance with the relevant legislation). This applies to both EU Member States and non-EEA states which are "equivalent jurisdictions".

Countries that meet the provisions in Regulations 13 and 17 are described as "equivalent jurisdictions". UK firms therefore need to determine whether a particular jurisdiction is 'equivalent', in order that it may take advantage of the SDD derogation, and/or to determine whether they may rely, for the purposes of carrying out CDD measures, on firms situated in a non-EEA state.

However, 'equivalence' only provides an exemption from the application of CDD measures, in respect of customer identification. It does not exempt the firm from carrying out ongoing monitoring of the business relationship with the customer, nor from the need for such other procedures (such as monitoring) as may be necessary to enable a firm to fulfil its responsibilities under the Proceeds of Crime Act 2002.

Although the judgement on equivalence is one to be made by each firm in the light of the particular circumstances, senior management is accountable for this judgement – either to its regulator, or, if necessary, to a court. It is therefore important that the reasons for concluding that a particular jurisdiction is equivalent (other than those in respect of which a presumption of equivalence may be made) are documented at the time the decision is made, and that it is made on relevant and up to date data or information.

## 2.2 Categories of country

### (a) Countries for which equivalence may be presumed

Jurisdictions where a presumption of equivalence may be made are:

- EU/EEA member states, through the implementation of the money laundering directive
- Countries on a list of equivalent jurisdictions issued by the EU, or by HMT

#### EU/EEA member states

Member States of the EU/EEA benefit de jure from mutual recognition through the implementation of the money laundering directive.

All Member States of the EU (which, for this purpose, includes Gibraltar as part of the UK, and Aruba as part of the Kingdom of the Netherlands) are required to enact legislation and financial sector procedures in accordance with the money laundering directive. In addition, EU Member States that are part of the Financial Action Task Force (FATF) have committed themselves to implementing the Forty Recommendations, and the Nine Special Recommendations to Combat Terrorist Financing.

All EEA countries have undertaken to implement the money laundering directive, and some are also FATF member countries.

#### *EU members of FATF:*

Austria	Ireland
Belgium	Italy
Denmark	Luxembourg
Finland	Netherlands
France	Portugal
Germany	Spain
Greece	Sweden

#### *Other EU member states:*

Bulgaria	Lithuania
Cyprus	Malta
Czech Republic	Poland
Estonia	Romania
Hungary	Slovakia
Latvia	Slovenia

#### *EEA states:*

Iceland - Member of FATF  
 Liechtenstein  
 Norway - Member of FATF

Although firms may initially presume equivalence, significant variations may exist in the precise measures (and in the timing of their introduction) that have been taken to transpose the money laundering directive (and its predecessors) into national laws and regulations. Moreover, the standards of compliance monitoring in respect of credit and financial institutions will also vary. Where firms have substantive information which indicates that a presumption of equivalence cannot be sustained, either in general or for particular products, they will need to consider whether their procedures should be enhanced to take account of this information.

**Deleted:** It would not normally be appropriate to make a presumption of equivalence in respect of other countries without further investigation.¶

The status of implementation of the money laundering directive across the EU is available at [http://ec.europa.eu/internal\\_market/company/docs/official/080522web\\_en.pdf](http://ec.europa.eu/internal_market/company/docs/official/080522web_en.pdf)

#### *EU agreed list*

Member states participating in the EU Committee on the Prevention of Money Laundering and Terrorist Financing have agreed a list of equivalent third countries, for the purposes of the relevant parts of the money laundering directive. The list is a voluntary, non-binding measure that nevertheless represents the common understanding of Member States. The text of the statement on equivalence and the list of equivalent jurisdictions are available at [http://ec.europa.eu/internal\\_market/company/financial-crime/index\\_en.htm#3rdcountry](http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm#3rdcountry).

The following third countries are currently considered as having equivalent AML/CTF systems to the EU. The list may be reviewed, in particular in the light of public evaluation reports adopted by the FATF, FSRBs, the IMF or the World Bank according to the revised 2003 FATF Recommendations and Methodology.

Australia	Mexico
Brazil	The Russian Federation
Canada	Singapore
Hong Kong	South Africa
India	Switzerland
Japan	The United States
<u>Republic of Korea</u>	

All of the above are members of the FATF.

The list also includes certain **French overseas territories** (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) and the **Dutch overseas territories** (Aruba). Those overseas territories are not members of the EU/EEA but are part of the membership of France and the Kingdom of the Netherlands of the FATF.

The **UK Crown Dependencies** (Jersey, Guernsey, Isle of Man) may also be considered as equivalent by Member States. **Gibraltar** is also directly subject to the requirements of the money laundering directive, which it has implemented. It is therefore considered to be equivalent for these purposes.

Firms should note that inclusion on the EU list does not override the need for firms to continue to operate risk-based procedures when dealing with customers based in an equivalent jurisdiction.

#### **(b) Countries for which equivalence should not be presumed**

It would not normally be appropriate to make a presumption of equivalence in respect of other countries without further investigation, notwithstanding that they might be members of other AML/CTF-related bodies.

#### *FATF members*

All FATF members (those which are not EU/EEA member states/countries are listed below) undertake to implement the FATF anti-money laundering and counter-terrorism Recommendations as part of their membership obligations.

However, unlike the transposition of the money laundering directive by EU Member States, implementation cannot be mandatory, and all members will approach their obligations in different ways, and under different timetables. Only those countries listed above under the EU agreed list may be presumed to be equivalent. The others are as follows:

- [Argentina](#)
- [China](#)
- [New Zealand](#)
- [Turkey](#)

**Deleted:** Argentina . . . . .  
 Mexico . . . . .  
 Australia . . . . . New Zealand . . . . .  
 Brazil . . . . . Russian Federation . . . . .  
 Canada . . . . . Singapore ¶  
 China . . . . . South Africa . . . . .  
 Hong Kong . . . . . Switzerland ¶  
 India . . . . . Turkey . . . . .  
 Japan . . . . . United States of America ¶  
 Republic of Korea . . . . . ¶  
 . . . . .

Information on the effectiveness of implementation in these jurisdictions may be obtained through scrutiny of Mutual Evaluation reports, which are published on the FATF website.

**Deleted:** in particular

*Gulf Co-operation Council*

The Gulf Co-operation Council (GCC) is in the unique position of being a member of FATF but with non-FATF countries as its members. However, whilst the GCC countries - Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates - have all undergone FATF-style mutual evaluations, few of these reports are publicly available. Moreover, few GCC countries have yet enacted legislation that contains equivalent provisions to the Money Laundering Directive, and so there is unevenness in the position of relevant regulation across GCC member countries. Individual GCC member countries should therefore be assessed in the same way as for other non-EU/FATF jurisdictions.

**Deleted:** ¶  
 All FATF members other than China, India, Republic of Korea and Turkey (and the Gulf Co-operation Council) are included in the EU list of equivalent jurisdictions referred to above.¶

None of the GCC members is included on the EU agreed lists, so there can be no presumption of equivalence.

*Other jurisdictions*

A majority of countries and territories do not fall within the lists of countries that can be presumed to be "equivalent jurisdictions". This does not necessarily mean that the AML/CTF legislation, and standards of due diligence, in those countries are lower than those in "equivalent jurisdictions". However, standards vary significantly, and firms will need to carry out their own assessment of particular countries. In addition to a firm's own knowledge and experience of the country concerned, particular attention should be paid to any FATF-style or IMF/World Bank evaluations that have been undertaken.

**Deleted:** ; this includes China, India, Republic of Korea and Turkey, which are all FATF members

As a result of due diligence carried out, therefore, jurisdictions may be added to those on the EU agreed list, for the purposes of determining those jurisdictions which, in the firm's judgement, are equivalent, for the purposes of the SDD derogation, and/or determining whether firms may rely, for the purposes of carrying out CDD measures, on other firms situated in such a jurisdiction.

**2.3 Factors to be taken into account when assessing other jurisdictions**

Factors include:

- Membership of groups that only admit those meeting a certain benchmark
- Contextual factors – political stability; level of (endemic) corruption etc
- Evidence of relevant (public) criticism of a jurisdiction, including HMT/FATF advisory notices
- Independent and public assessment of the jurisdiction's overall AML regime
- Need for any assessment to be recent
- Implementation standards (inc quality and effectiveness of supervision)

- Incidence of trade with the jurisdiction – need to be proportionate especially where very small

*Membership of an international or regional ‘group’*

There are a number of international and regional ‘groups’ of jurisdictions that admit to membership only those jurisdictions that have demonstrated a commitment to the fight against money laundering and terrorist financing, and which have an appropriate legal and regulatory regime to back up this commitment.

*Contextual factors*

Such factors as the political stability of a jurisdiction, and where it stands in tables of corruption are relevant to whether it is likely that a jurisdiction will be ‘equivalent’. It will, however, seldom be easy for firms to make their own assessments of such matters, and it is likely that they will have to rely on external agencies for such evidence – whether prepared for general consumption, or specifically for the firm. Where the firm looks to publicly available evidence, it will be important that it has some knowledge of the criteria that were used in making the assessment; the firm cannot rely solely on the fact that such a list has been independently prepared, even if by a respected third party agency.

*Evidence of relevant (public) criticism*

The FATF from time to time issues statements on its concerns about the lack of comprehensive AML/CFT systems in a number of jurisdictions (see section 2.4 below). When constructing their internal procedures, therefore, financial sector firms should have regard to the need for additional monitoring procedures for transactions from any country that is listed on these statements of concern. Additional monitoring procedures will also be required in respect of correspondent relationships with financial institutions from such countries.

Other, commercial agencies also produce reports and lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CTF area. Such reports lists can provide some useful and relevant evidence – which may or may not be conclusive – on whether or not a particular jurisdiction is likely to be equivalent.

*Mutual evaluation reports*

Particular attention should be paid to assessments that have been undertaken by standard setting bodies such as FATF, and by international financial institutions such as the IMF.

FATF

FATF member countries monitor their own progress in the fight against money laundering and terrorist financing through regular mutual evaluation by their peers. In 1998, FATF extended the concept of mutual evaluation beyond its own membership through its endorsement of FATF-style mutual evaluation programmes of a number of regional groups which contain non-FATF members. The groups undertaking FATF-style mutual evaluations are

- the Offshore Group of Banking Supervisors (OGBS) see [www.ogbs.net](http://www.ogbs.net)
- the Caribbean Financial Action Task Force (CFATF) see [www.cfatf.org](http://www.cfatf.org)
- the Asia/Pacific Group on Money Laundering (APG) see [www.apgml.org](http://www.apgml.org)
- MONEYVAL, covering the Council of Europe countries which are not members of FATF see [www.coe.int/moneyval](http://www.coe.int/moneyval)
- the Financial Action Task Force on Money Laundering in South America (GAFISUD) see [www.gafisud.org](http://www.gafisud.org)
- the Middle East and North Africa Financial Action Task Force (MENAFATF) see [www.menafatf.org](http://www.menafatf.org)
- the Eurasian Group (EAG) see [www.eurasiangroup.org](http://www.eurasiangroup.org).

- the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) see [www.esaamlg.org](http://www.esaamlg.org)
- the Intergovernmental Action Group against Money-Laundering in Africa (GIABA) see [www.giabasn.org](http://www.giabasn.org)

Firms should bear in mind that mutual evaluation reports are at a 'point in time', and should be interpreted as such. Although follow up actions are usually reviewed after two years, there can be quite long intervals between evaluation reports in respect of a particular jurisdiction. Even at the point an evaluation is carried out there can be changes in train to the jurisdiction's AML/CTF regime, but these will not be reflected in the evaluation report. There can also be subsequent changes to the regime (whether to respond to criticisms by the evaluators or otherwise) which firms should seek to understand and to factor into their assessment of whether the jurisdiction is equivalent.

In assessing the conclusions of a mutual evaluation report, firms may find it difficult to give appropriate weighting to findings and conclusions in respect of the jurisdiction's compliance with particular Recommendations. For the purposes of assessing equivalence, compliance (or otherwise) with certain Recommendations may have more relevance than others. The extent to which a jurisdiction complies with the following Recommendations may be particularly relevant:

*Legal framework:*

Recommendation 1  
Special Recommendation II

*Measures to be taken by firms:*

Recommendations 4, 5, 6, 9, 10, 11, and 13,  
Special Recommendation IV

*Supervisory regime:*

Recommendations 17, 23, 29 and 30

*International co-operation:*

Recommendation 40

Summaries of FATF and FATF-style evaluations are published in FATF Annual Reports and can be accessed at [www.fatf-gafi.org](http://www.fatf-gafi.org). However, mutual evaluation reports prepared by some FATF-style regional bodies may not be carried out fully to FATF standards, and firms should bear this in mind if a decision on whether a jurisdiction is equivalent is based on such reports.

**IMF/World bank**

As part of their financial stability assessments of countries and territories, the IMF and the World Bank have agreed with FATF a detailed methodology for assessing compliance with AML/CTF standards, using the FATF Recommendations as the base. A number of countries have already undergone IMF/World Bank assessments in addition to those carried out by FATF, and some of the results can be accessed at [www.imf.org](http://www.imf.org). Where IMF/World Bank assessments relate to FATF members, the assessments are formally adopted by the FATF and appear on the FATF website.

*Implementation standards (including effectiveness of supervision)*

Information on the extent and quality of supervision of AML/CTF standards may be obtained from the extent to which a jurisdiction complies with Recommendations 17, 23, 29 and 30.

*Incidence of trade with the jurisdiction*

In respect of any particular jurisdiction, the level and extent of due diligence that needs to be carried out in making a judgement on equivalence will be influenced by the volume and size of the firm's business with that jurisdiction in relation to the firm's overall business.

## 2.4 UK prohibition notices and advisory notices

### *Prohibition notices*

As at ~~December 2011~~, no prohibition notices have been issued by HM Treasury under Regulation 18 of the 2007 Regulations.

Deleted: October

### *Advisory notices*

#### *HM Treasury*

HM Treasury issues press notices in which it expresses the UK's full support of the work of the FATF on jurisdictions of concern. The HM Treasury press notices are available at <http://www.hm-treasury.gov.uk/press>

The FATF issues periodic announcements about its concerns regarding the lack of comprehensive AML/CFT systems in various jurisdictions.

The FATF maintains a *Public Statement* which lists jurisdictions of concern in three categories:

1. Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing (ML/TF) risks emanating from the jurisdiction.
2. Jurisdictions with strategic AML/CFT deficiencies that have not committed to an action plan developed with the FATF to address key deficiencies. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below.
3. Jurisdictions previously publicly identified by the FATF as having strategic AML/CFT deficiencies, which remain to be addressed.

The FATF also maintains a statement *Improving Global AML/CFT Compliance: On-going Process*, which lists jurisdictions identified as having strategic AML/CFT deficiencies for which they have developed an action plan with the FATF. While the situations differ among jurisdictions, each has provided a written high-level political commitment to address the identified deficiencies. The FATF will closely monitor the implementation of these action plans and encourages its members to consider the information set out in the statement.

The latest versions of these FATF Statements are available at <http://www.fatf-gafi.org>.

#### *FSA*

The FSA has set out how it expects firms to use information contained in the FATF Public Statements:

“The FSA expects authorised firms to establish and maintain systems and controls to counter the risk that they might be used to further financial crime. All firms must also comply with their legal obligations under the Money Laundering Regulations 2007. We would therefore expect all firms to actively consider the risks associated with transactions and business relationships linked to

jurisdictions included within these statements. Policies and procedures must be adapted where necessary to reflect this.

“We also expect firms supervised by the FSA for money laundering purposes to consider the impact of these statements on their policies and procedures in relation to simplified due diligence under section 13 and reliance under section 17 of the Money Laundering Regulations 2007”.

### 3: Equivalent markets

*This material is issued to assist firms by setting out how they might approach their assessment of regulated markets, to determine whether they are 'equivalent' for the purposes of the money laundering directive. Although it is not formal guidance that has been given Ministerial approval, it has been discussed with HM Treasury and reflects their input.*

*The material discusses markets where there may be a presumption of equivalence and those where such a presumption may not be appropriate without further investigation. It then discusses issues that a firm should consider in all cases when coming to a judgement on whether a particular market is, in its view, equivalent.*

#### 3.1 What is an "equivalent market" and why does it matter?

The 3rd European Council Directive on prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the money laundering directive) allows firms (article 11) to carry out simplified due diligence (SDD) in respect of customers whose securities are

- listed on a regulated market, which is
- subject to specified disclosure obligations.

The Money Laundering Regulations 2007 (the 2007 Regulations) implement the provisions of the money laundering directive into UK law, and accordingly provide (Regulation 13) that firms may apply SDD to customers whose securities are listed on a regulated market that is subject to specified disclosure obligations [See section 3.2 and Annex 3-II].

Under the 2007 Regulations (and the money laundering directive), a "regulated market"

- within the EEA has the meaning given by point 14 of Article 4(1) of the markets in financial instruments directive (MiFID). [This definition is reproduced in Annex 3-I].
- outside the EEA, means a regulated financial market which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations [see section 3.2 and Annex 3-II]

Markets that meet the definition in the 2007 Regulations are described in the JMLSG Guidance as "equivalent markets". UK firms therefore need to determine whether a particular market is 'equivalent', in order that they may take advantage of the SDD derogation. If a market does not qualify as 'equivalent', or if a firm chooses not to determine whether the market is 'equivalent', full CDD measures must be applied to the customer.

However, 'equivalence' only provides an exemption from the application of CDD measures in respect of customer identification. It does not exempt the firm from carrying out ongoing monitoring of the business relationship with the customer, nor from the need for such other procedures (such as monitoring) as may be necessary to enable a firm to fulfil its responsibilities under the Proceeds of Crime Act 2002.

Although the judgement on equivalence of regulated markets is one to be made by each firm in the light of the particular circumstances of the market, senior management is accountable for this judgement – either to its regulator, or, if necessary, to a court. It is therefore important that the reasons for concluding that a particular market is equivalent (other than those in respect of which a presumption of equivalence may be made) are documented at the time the decision is made, and that it is made on relevant and up to date data or information.

### 3.2 What are the specified disclosure obligations?

The disclosure obligations that the 2007 Regulations require regulated markets to impose are those consistent with

- Article 6(1) to (4) of Directive 2003/6/EC [the Market Abuse Directive];
- Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC [the Prospectus Directive];
- Articles 4 to 6, 14, 16 to 19 and 30 of Directive 2004/109/EC [the Transparency Directive]; and
- Community legislation made under the above provisions.

These obligations are reproduced at Annex 3-II.

### 3.3 Categories of market

#### *Markets in EU/EEA member states*

All Member States of the EU (which, for this purpose, includes Gibraltar as part of the UK, and Aruba as part of the Kingdom of the Netherlands) are required to enact legislation and regulations in accordance with the specified disclosure obligations. All EEA countries have undertaken to implement the directives from which the specified disclosure obligations flow.

ESMA maintains a database of regulated markets within the EU (this is not, of course, a formal list of “equivalent” markets). The list is published for the purpose of identification of the counterparty to the transaction in relation to transaction reporting. Publication of the identifiers ensures the compliance of ESMA members with Article 13 (2) of the MiFID Level 2 regulation. ESMA has collected this information from its members and will update the list on a regular basis. Some ESMA members will, in addition, publish their own information separately on their websites. Further information is available on the ESMA website at <http://mifiddatabase.esma.eu/>.

Generally, the *principal* markets in EU/EEA member states are likely to be able to be presumed to be ‘equivalent’ for the purposes of the 2007 Regulations. In the 2007 Regulations, however, it was chosen to link the derogation to the admission to listing in a regulated market within the meaning of MiFID. So listing in other markets (such as AIM<sup>2</sup>) would not be enough qualification for the application of the derogation.

#### *Markets in some third countries*

Outside the EEA, a regulated financial market is ‘equivalent’ for the purposes of the 2007 Regulations if it subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations. Article 19(6) of MiFID [see Annex 3-I] requires the Commission to publish a list of third country markets that are ‘equivalent’ under MiFID.

A firm might reasonably conclude that a regulated market that is equivalent for MiFID purposes will be equivalent for the purposes of the 2007 Regulations. Some other third country markets might still meet

---

<sup>2</sup> But see paragraph 5.3.135 in Part I of the Guidance, which suggests that the due process for admission to AIM may give equivalent comfort.

the requirements of the money laundering directive, however, even although they do not meet all those required by MiFID.

The Commission has not yet published a list of equivalent third country markets for MiFID purposes; when it does, these may reasonably be regarded as equivalent for the purposes of the 2007 Regulations, whilst leaving it open for other individual markets also to be recognised for the purposes of the 2007 Regulations.

*Caveat... ..*

Although firms may rely on the presumption of equivalence, in respect of certain markets significant variations may exist in the precise measures (and in the timing of their introduction) that have been taken to transpose the obligations under the various directives into national laws and market regulations. Moreover, the standards of compliance monitoring in respect of particular markets will also vary. Where firms have substantive information which indicates that a presumption of equivalence cannot be sustained, either in general or for particular markets, they will need to apply full CDD measures to customers listed on these markets.

The status of implementation of the relevant directives across the EU is available at [http://ec.europa.eu/internal\\_market/securities/transposition/index\\_en.htm](http://ec.europa.eu/internal_market/securities/transposition/index_en.htm).

*Other markets*

Although markets in other countries and territories cannot be presumed to be "equivalent", this does not necessarily mean that the legislation and disclosure obligations in those countries are lower than those in "equivalent markets". However, standards vary significantly, and firms will need to carry out their own assessment of the transparency and disclosure obligations in these particular markets. In addition to a firm's own knowledge and experience of the market concerned, particular attention should be paid to any evaluations or analyses of disclosure obligations that have been undertaken.

### **3.4 Factors to be taken into account when assessing other markets**

The primary consideration that firms should address initially as part of their assessment is whether the disclosure and other obligations in a particular market meet the disclosure obligations specified in the directive.

*Do the obligations in the particular market meet the specified disclosure obligations?*

The money laundering directive is open on the extent to which disclosures in third countries must be sufficiently consistent with Community legislation to enable them to be regarded as 'equivalent'. On one interpretation, a firm could require that *all* provisions in the relevant directives must be faithfully reflected in the third country market obligations. However, a more workable interpretation is that it is enough to satisfy the major provisions in the relevant directives.

Commission Directive 2007/14/EC (the MiFID Implementing Directive) contains some provisions (Articles 13 to 23) on how to judge the equivalence of third country rules regarding some obligations of the Transparency Directive. Recital 18 of this directive provides a helpful definition of equivalence:

*(18) Equivalence should be able to be declared when general disclosure rules of third countries provide users with understandable and broadly equivalent assessment of issuers' position that enable them to make similar decisions as if they were provided with the information according to requirements under Directive 2004/109/EC, even if the requirements are not identical. ... ..*

It is important to note that the country of incorporation of the company is of little relevance. What counts is that it is subject to appropriate disclosure requirements in an equivalent market, which may well be in a different jurisdiction.

*Other relevant matters to consider*

Other relevant factors in making an assessment of 'equivalence' include:

- Membership of groups that only admit those meeting certain criteria
- Contextual factors – political stability; level of (endemic) corruption etc
- Evidence of relevant (public) criticism of a market
- Independent and public assessment of the market’s overall disclosure and transparency standards
- Need for any assessment to be recent
- Implementation standards (including quality and effectiveness of supervision)

Membership of an international or regional ‘group’

There are a number of international and regional ‘groups’ of markets that admit to membership only those markets that have demonstrated a commitment to high standards of disclosure and transparency, and which have an appropriate legal and regulatory regime to back up this commitment. Where a market is a member of such a group, there may be a presumption that the market is likely to be ‘equivalent’.

Contextual factors

Such factors as the political stability of the jurisdiction within which a market is located, and where it stands in tables of corruption are relevant to whether it is likely that a market will be ‘equivalent’. It will, however, seldom be easy for firms to make their own assessments of such matters, and it is likely that they will have to rely on external agencies for such evidence – whether prepared for general consumption, or specifically for the firm.

Evidence of relevant (public) criticism

Commercial agencies and the media also produce reports and lists of markets, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity. Such reports lists can provide some useful and relevant evidence – which may or may not be conclusive – on whether or not a particular market is likely to be equivalent.

Independent reports on disclosure and transparency standards

Particular attention should be paid to assessments of particular markets, including their disclosure and transparency standards, which have been undertaken by respected third party agencies. Where the firm looks to publicly available evidence, it will be important that it has some knowledge of the criteria that were used in making the assessment; the firm cannot rely solely on the fact that such an assessment has been independently prepared.

It should be noted that, under the Transparency Directive framework (notably Article 23(1)), declaring equivalence of third country regimes is a task for the national financial services supervisors: i.e., FSA in the UK.

Implementation standards (including effectiveness of supervision)

Information on the extent and quality of supervision of markets may be published by the competent authorities – whether in annual reports or otherwise.

## ANNEX 3-I

**RELEVANT PROVISIONS OF MiFID****Definition of ‘regulated market’****Point 14 of Article 4(1):**

“Regulated market” means a multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments – in the system and in accordance with its non-discretionary rules – in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with the provisions of Title III [of MiFID]

**Title III includes the following (Article 40):**

- |  |  |
|--|--|
| <i>Markets must have clear and transparent rules</i>   | 1. Member States shall require that regulated markets have clear and transparent rules regarding the admission of financial instruments to trading. Those rules shall ensure that any financial instruments admitted to trading in a regulated market are capable of being traded in a fair, orderly and efficient manner and, in the case of transferable securities, are freely negotiable.  |
| <i>Design of contracts must allow for orderly pricing</i>  | 2. In the case of derivatives, the rules shall ensure in particular that the design of the derivative contract allows for its orderly pricing as well as for the existence of effective settlement conditions.   |
| <i>Markets must establish arrangements to verify issuers’ compliance with disclosure obligations</i> | 3. In addition to the obligations set out in paragraphs 1 and 2, Member States shall require the regulated market to establish and maintain effective arrangements to verify that issuers of transferable securities that are admitted to trading on the regulated market comply with their obligations under Community law in respect of initial, ongoing or ad hoc disclosure obligations. Member States shall ensure that the regulated market establishes arrangements which facilitate its members or participants in obtaining access to information which has been made public under Community law. |
| <i>Markets must be subject to regulatory oversight</i>   | 4. Member States shall ensure that regulated markets have established the necessary arrangements to review regularly the compliance with the admission requirements of the financial instruments which they admit to trading.  |

**Commission obligation to publish a list of third country markets considered as equivalent**

**Article 19:**

...

(6) Member States shall allow investment firms when providing investment services that only consist of execution [ ..... ] to provide those investment services to their clients without the need to obtain the information or make the determination provided for in paragraph 5 [*appropriateness test*] where all the following conditions are met:

- the above services relate to shares admitted to trading on a regulated market or in an equivalent third country market, [ ..... ]. A third country market shall be considered as equivalent to a regulated market if it complies with equivalent requirements to those established under Title III. The Commission shall publish a list of those markets that are to be considered as equivalent. This list shall be updated periodically.

## ANNEX 3-II

**DETAILS OF THE “SPECIFIED DISCLOSURE OBLIGATIONS” REFERRED TO IN  
2007 REGULATIONS**

***DIRECTIVE 2003/6/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 28 January 2003 on insider dealing and market manipulation (Market Abuse Directive)***

## Article 6

*All relevant inside  
information must  
be disclosed*

1. Member States shall ensure that issuers of financial instruments inform the public as soon as possible of inside information which directly concerns the said issuers. Without prejudice to any measures taken to comply with the provisions of the first subparagraph, Member States shall ensure that issuers, for an appropriate period, post on their Internet sites all inside information that they are required to disclose publicly.

*Delay in publishing  
inside information  
must not mislead  
the public*

2. An issuer may under his own responsibility delay the public disclosure of inside information, as referred to in paragraph 1, such as not to prejudice his legitimate interests provided that such omission would not be likely to mislead the public and provided that the issuer is able to ensure the confidentiality of that information. Member States may require that an issuer shall without delay inform the competent authority of the decision to delay the public disclosure of inside information.

*Inside information  
disclosed to a third  
party must be  
published  
simultaneously*

3. Member States shall require that, whenever an issuer, or a person acting on his behalf or for his account, discloses any inside information to any third party in the normal exercise of his employment, profession or duties, as referred to in Article 3(a), he must make complete and effective public disclosure of that information, simultaneously in the case of an intentional disclosure and promptly in the case of a non-intentional disclosure. The provisions of the first subparagraph shall not apply if the person receiving the information owes a duty of confidentiality, regardless of whether such duty is based on a law, on regulations, on articles of association or on a contract. Member States shall require that issuers, or persons acting on their behalf or for their account, draw up a list of those persons working for them, under a contract of employment or otherwise, who have access to inside information. Issuers and persons acting on their behalf or for their account shall regularly update this list and transmit it to the competent authority whenever the latter requests it.

*Transactions of  
individual members  
of management in  
an issuer's shares  
must be publicly  
disclosed as soon  
as possible*

4. Persons discharging managerial responsibilities within an issuer of financial instruments and, where applicable, persons closely associated with them, shall, at least, notify to the competent authority the existence of transactions conducted on their own account relating to shares of the said issuer, or to derivatives or other financial instruments linked to them. Member States shall ensure that public access to information concerning such transactions, on at least an individual basis, is readily available as soon as possible.

***DIRECTIVE 2003/71/EC OF THE EUROPEAN PARLIAMENT AND OF THE  
COUNCIL  
of 4 November 2003 on the prospectus to be published when securities are offered  
to the public or admitted to trading and amending Directive 2001/34/EC***

***(Prospectus Directive)***

*Public offerings of a security must not be allowed without prior publication of a prospectus*

*Types of offer that do not need to be accompanied by a prospectus*

*Admission of securities to trading on a regulated market must be subject to publication of a prospectus*

### Article 3

#### Obligation to publish a prospectus

1. Member States shall not allow any offer of securities to be made to the public within their territories without prior publication of a prospectus.

2. The obligation to publish a prospectus shall not apply to the following types of offer:

- (a) an offer of securities addressed solely to qualified investors; and/or
- (b) an offer of securities addressed to fewer than 100 natural or legal persons per Member State, other than qualified investors; and/or
- (c) an offer of securities addressed to investors who acquire securities for a total consideration of at least EUR 50000 per investor, for each separate offer; and/or
- (d) an offer of securities whose denomination per unit amounts to at least EUR 50000; and/or
- (e) an offer of securities with a total consideration of less than EUR 100000, which limit shall be calculated over a period of 12 months.

However, any subsequent resale of securities which were previously the subject of one or more of the types of offer mentioned in this paragraph shall be regarded as a separate offer and the definition set out in Article 2(1)(d) shall apply for the purpose of deciding whether that resale is an offer of securities to the public. The placement of securities through financial intermediaries shall be subject to publication of a prospectus if none of the conditions (a) to (e) are met for the final placement.

3. Member States shall ensure that any admission of securities to trading on a regulated market situated or operating within their territories is subject to the publication of a prospectus.

### Article 5

*Prospectuses shall contain all the information necessary to enable investors to make informed decisions*

The prospectus

1. Without prejudice to Article 8(2), the prospectus shall contain all information which, according to the particular nature of the issuer and of the securities offered to the public or admitted to trading on a regulated market, is necessary to enable investors to make an informed assessment of the assets and liabilities, financial position, profit and losses, and prospects of the issuer and of any guarantor, and of the rights attaching to such securities. This information shall be presented in an easily analysable and comprehensible form.

*Prospectuses must contain a summary in brief and non-technical language...*

2. The prospectus shall contain information concerning the issuer and the securities to be offered to the public or to be admitted to trading on a regulated market. It shall also include a summary. The summary shall, in a brief manner and in non-technical language, convey the essential characteristics and risks associated with the issuer, any guarantor and the securities, in the language in which the prospectus was originally drawn up. The summary shall also contain a warning that:

*with appropriate warnings...*

(a) it should be read as an introduction to the prospectus;  
 (b) any decision to invest in the securities should be based on consideration of the prospectus as a whole by the investor;  
 (c) where a claim relating to the information contained in a prospectus is brought before a court, the plaintiff investor might, under the national legislation of the Member States, have to bear the costs of translating the prospectus before the legal proceedings are initiated; and  
 (d) civil liability attaches to those persons who have tabled the summary including any translation thereof, and applied for its notification, but only if the summary is misleading, inaccurate or inconsistent when read together with the other parts of the prospectus. Where the prospectus relates to the admission to trading on a regulated market of non-equity securities having a denomination of at least EUR 50000, there shall be no requirement to provide a summary except when requested by a Member State as provided for in Article 19(4).

*A prospectus may be a single document or three separate documents*

3. Subject to paragraph 4, the issuer, offeror or person asking for the admission to trading on a regulated market may draw up the prospectus as a single document or separate documents. A prospectus composed of separate documents shall divide the required information into a registration document, a securities note and a summary note. The registration document shall contain the information relating to the issuer. The securities note shall contain the information concerning the securities offered to the public or to be admitted to trading on a regulated market.

4. For the following types of securities, the prospectus can, at the choice of the issuer, offeror or person asking for the admission to trading on a regulated market consist of a base prospectus containing all relevant information concerning the issuer and the securities offered to the public or to be admitted to trading on a regulated market:

- (a) non-equity securities, including warrants in any form, issued under an offering programme;
- (b) non-equity securities issued in a continuous or repeated manner by credit institutions,
- (i) where the sums deriving from the issue of the said securities, under national legislation, are placed in assets which provide sufficient coverage for the liability deriving from securities until their maturity date;
- (ii) where, in the event of the insolvency of the related credit institution, the said sums are intended, as a priority, to repay the capital and interest falling due, without prejudice to the provisions of Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions (14). The information given in the base prospectus shall be supplemented, if necessary, in accordance with Article 16, with updated information on the issuer and on the securities to be offered to the public or to be admitted to trading on a regulated market. If the final terms of the offer are not included in either the base prospectus or a supplement, the final terms shall be provided to investors and filed with the competent authority when each public offer is made as soon as practicable and if possible in advance of the beginning of the offer. The provisions of Article 8(1)(a) shall be applicable in any such case.

*In certain cases, a prospectus can be a 'base prospectus'*

5. In order to take account of technical developments on financial markets and to ensure uniform application of this Directive, the Commission shall, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning the format of the prospectus or base prospectus and supplements.

*The Commission shall adopt implementing measures concerning the format of a prospectus*

## Article 7

## Minimum information

*The Commission shall adopt implementing measures regarding the specific information to be included in a prospectus*

1. Detailed implementing measures regarding the specific information which must be included in a prospectus, avoiding duplication of information when a prospectus is composed of separate documents, shall be adopted by the Commission in accordance with the procedure referred to in Article 24(2). The first set of implementing measures shall be adopted by 1 July 2004.

2. In particular, for the elaboration of the various models of prospectuses, account shall be taken of the following:

(a) the various types of information needed by investors relating to equity securities as compared with non-equity securities; a consistent approach shall be taken with regard to information required in a prospectus for securities which have a similar economic rationale, notably derivative securities;

(b) the various types and characteristics of offers and admissions to trading on a regulated market of non-equity securities. The information required in a prospectus shall be appropriate from the point of view of the investors concerned for non-equity securities having a denomination per unit of at least EUR 50000;

(c) the format used and the information required in prospectuses relating to non-equity securities, including warrants in any form, issued under an offering programme;

(d) the format used and the information required in prospectuses relating to non-equity securities, in so far as these securities are not subordinated, convertible, exchangeable, subject to subscription or acquisition rights or linked to derivative instruments, issued in a continuous or repeated manner by entities authorised or regulated to operate in the financial markets within the European Economic Area;

(e) the various activities and size of the issuer, in particular SMEs. For such companies the information shall be adapted to their size and, where appropriate, to their shorter track record;

(f) if applicable, the public nature of the issuer.

3. The implementing measures referred to in paragraph 1 shall be based on the standards in the field of financial and non-financial information set out by international securities commission organisations, and in particular by IOSCO and on the indicative Annexes to this Directive.

*The Commission's implementing measures shall be based on IOSCO standards....*

## Article 8

## Omission of information

*Conditions under which certain information may be omitted.....*

1. Member States shall ensure that where the final offer price and amount of securities which will be offered to the public cannot be included in the prospectus: (a) the criteria, and/or the conditions in accordance with which the above elements will be determined or, in the case of price, the maximum price, are disclosed in the prospectus; or (b) the acceptances of the purchase or subscription of securities may be withdrawn for not less than two working days after the final offer price and amount of securities which will be offered to the public have been filed. The final offer price and amount of securities shall be filed with the competent authority of the home Member State and published in accordance with the arrangements provided for in Article 14(2).

*Circumstances under which the competent authority may authorize omission of certain information.....*

2. The competent authority of the home Member State may authorise the omission from the prospectus of certain information provided for in this Directive or in the implementing measures referred to in Article 7(1), if it considers that: (a) disclosure of such information would be contrary to the public interest; or (b) disclosure of such information would be seriously detrimental to the issuer, provided that the omission would not be likely to mislead the public with regard to facts and circumstances essential for an informed assessment of the issuer, offeror or guarantor, if any, and of the rights attached to the securities to which the prospectus relates; or (c) such information is of minor importance only for a specific offer or admission to trading on a regulated market and is not such as will influence the assessment of the financial position and prospects of the issuer, offeror or guarantor, if any.

*Conditions to be met where certain information required by implementing measures is inappropriate....*

3. Without prejudice to the adequate information of investors, where, exceptionally, certain information required by implementing measures referred to in Article 7(1) to be included in a prospectus is inappropriate to the issuer's sphere of activity or to the legal form of the issuer or to the securities to which the prospectus relates, the prospectus shall contain information equivalent to the required information. If there is no such information, this requirement shall not apply.

*The Commission shall adopt implementing measures concerning circumstances where omissions may be authorized...*

4. In order to take account of technical developments on financial markets and to ensure uniform application of this Directive, the Commission shall, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning paragraph 2.

## Article 10

## Information

*Issuers must provide an annual document referring to all information published in compliance with their obligations.....*

1. Issuers whose securities are admitted to trading on a regulated market shall at least annually provide a document that contains or refers to all information that they have published or made available to the public over the preceding 12 months in one or more Member States and in third countries in compliance with their obligations under Community and national laws and rules dealing with the regulation of securities, issuers of securities and securities markets. Issuers shall refer at least to the information required pursuant to company law directives, Directive 2001/34/EC and Regulation (EC) No 1606/2002 of the European Parliament and of the Council of 19 July 2002 on the application of international accounting standards (15).

*such document to be filed with the competent authority....*

2. The document shall be filed with the competent authority of the home Member State after the publication of the financial statement. Where the document refers to information, it shall be stated where the information can be obtained.

*circumstances where such a document is not required...*

3. The obligation set out in paragraph 1 shall not apply to issuers of non-equity securities whose denomination per unit amounts to at least EUR 50000.

*The Commission may adopt implementing measures relating to the method of publication of the document.....*

4. In order to take account of technical developments on financial markets and to ensure uniform application of this Directive, the Commission may, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning paragraph 1. These measures will relate only to the method of publication of the disclosure requirements mentioned in paragraph 1 and will not entail new disclosure requirements. The first set of implementing measures shall be adopted by 1 July 2004.

## Article 14

#### Publication of the prospectus

*Prospectus shall be filed with the competent authority and made available to the public....*

1. Once approved, the prospectus shall be filed with the competent authority of the home Member State and shall be made available to the public by the issuer, offeror or person asking for admission to trading on a regulated market as soon as practicable and in any case, at a reasonable time in advance of, and at the latest at the beginning of, the offer to the public or the admission to trading of the securities involved. In addition, in the case of an initial public offer of a class of shares not already admitted to trading on a regulated market that is to be admitted to trading for the first time, the prospectus shall be available at least six working days before the end of the offer.

*Meaning of 'available to the public'....*

2. The prospectus shall be deemed available to the public when published either:

- (a) by insertion in one or more newspapers circulated throughout, or widely circulated in, the Member States in which the offer to the public is made or the admission to trading is sought; or
- (b) in a printed form to be made available, free of charge, to the public at the offices of the market on which the securities are being admitted to trading, or at the registered office of the issuer and at the offices of the financial intermediaries placing or selling the securities, including paying agents; or
- (c) in an electronic form on the issuer's website and, if applicable, on the website of the financial intermediaries placing or selling the securities, including paying agents; or
- (d) in an electronic form on the website of the regulated market where the admission to trading is sought; or
- (e) in electronic form on the website of the competent authority of the home Member State if the said authority has decided to offer this service. A home Member State may require issuers which publish their prospectus in accordance with (a) or (b) also to publish their prospectus in an electronic form in accordance with (c).

3. In addition, a home Member State may require publication of a notice stating how the prospectus has been made available and where it can be obtained by the public.

*Member states may require publication of a notice stating where a prospectus may be obtained*

4. The competent authority of the home Member State shall publish on its website over a period of 12 months, at its choice, all the prospectuses approved, or at least the list of prospectuses approved in accordance with Article 13, including, if applicable, a hyperlink to the prospectus published on the website of the issuer, or on the website of the regulated market.

*Competent authority must publish all prospectuses approved, or a list with hyperlinks....*

5. In the case of a prospectus comprising several documents and/or incorporating information by reference, the documents and information making up the prospectus may be published and circulated separately provided that the said documents are made available, free of charge, to the public, in accordance with the arrangements established in paragraph 2. Each document shall indicate where the other constituent documents of the full prospectus may be obtained.

*Each document making up a prospectus may be published separately...*

*The text and format of the prospectus made available to the public must be the same as that filed...*

*If published electronically, paper copies must also be available...*

*The Commission shall adopt implementing measures concerning the publication of a prospectus*

6. The text and the format of the prospectus, and/or the supplements to the prospectus, published or made available to the public, shall at all times be identical to the original version approved by the competent authority of the home Member State.

7. Where the prospectus is made available by publication in electronic form, a paper copy must nevertheless be delivered to the investor, upon his request and free of charge, by the issuer, the offeror, the person asking for admission to trading or the financial intermediaries placing or selling the securities.

8. In order to take account of technical developments on financial markets and to ensure uniform application of the Directive, the Commission shall, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning paragraphs 1, 2, 3 and 4. The first set of implementing measures shall be adopted by 1 July 2004.

## Article 16

## Supplements to the prospectus

*Certain events taking place between publication of the prospectus and final closing of the offer must be mentioned in a supplement to the prospectus.....*

1. Every significant new factor, material mistake or inaccuracy relating to the information included in the prospectus which is capable of affecting the assessment of the securities and which arises or is noted between the time when the prospectus is approved and the final closing of the offer to the public or, as the case may be, the time when trading on a regulated market begins, shall be mentioned in a supplement to the prospectus. Such a supplement shall be approved in the same way in a maximum of seven working days and published in accordance with at least the same arrangements as were applied when the original prospectus was published. The summary, and any translations thereof, shall also be supplemented, if necessary to take into account the new information included in the supplement.

*Investors may withdraw their agreement to purchase if a supplement is published....*

2. Investors who have already agreed to purchase or subscribe for the securities before the supplement is published shall have the right, exercisable within a time limit which shall not be shorter than two working days after the publication of the supplement, to withdraw their acceptances.

***DIRECTIVE 2004/109/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC (Transparency Directive)***

Article 4

Annual financial reports

*Publication deadline for annual financial reports*

1. The issuer shall make public its annual financial report at the latest four months after the end of each financial year and shall ensure that it remains publicly available for at least five years.

2. The annual financial report shall comprise:

*Documents that shall comprise the annual financial report*

(a) the audited financial statements;  
(b) the management report; and  
(c) statements made by the persons responsible within the issuer, whose names and functions shall be clearly indicated, to the effect that, to the best of their knowledge, the financial statements prepared in accordance with the applicable set of accounting standards give a true and fair view of the assets, liabilities, financial position and profit or loss of the issuer and the undertakings included in the consolidation taken as a whole and that the management report includes a fair review of the development and performance of the business and the position of the issuer and the undertakings included in the consolidation taken as a whole, together with a description of the principal risks and uncertainties that they face.

*Where consolidated accounts are required....*

3. Where the issuer is required to prepare consolidated accounts according to the Seventh Council Directive 83/349/EEC of 13 June 1983 on consolidated accounts [15], the audited financial statements shall comprise such consolidated accounts drawn up in accordance with Regulation (EC) No 1606/2002 and the annual accounts of the parent company drawn up in accordance with the national law of the Member State in which the parent company is incorporated. Where the issuer is not required to prepare consolidated accounts, the audited financial statements shall comprise the accounts prepared in accordance with the national law of the Member State in which the company is incorporated.

*Requirement for financial statements to be audited....*

4. The financial statements shall be audited in accordance with Articles 51 and 51a of the Fourth Council Directive 78/660/EEC of 25 July 1978 on the annual accounts of certain types of companies [16] and, if the issuer is required to prepare consolidated accounts, in accordance with Article 37 of Directive 83/349/EEC. The audit report, signed by the person or persons responsible for auditing the financial statements, shall be disclosed in full to the public together with the annual financial report.

*Requirement for a  
management report...*

5. The management report shall be drawn up in accordance with Article 46 of Directive 78/660/EEC and, if the issuer is required to prepare consolidated accounts, in accordance with Article 36 of Directive 83/349/EEC.

*The Commission shall  
adopt implementing  
measures concerning  
the publication of  
annual financial  
reports*

6. The Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets and to ensure the uniform application of paragraph 1. The Commission shall in particular specify the technical conditions under which a published annual financial report, including the audit report, is to remain available to the public. Where appropriate, the Commission may also adapt the five-year period referred to in paragraph 1.

## Article 5

*Requirement for half-yearly financial reports....*

#### Half-yearly financial reports

1. The issuer of shares or debt securities shall make public a half-yearly financial report covering the first six months of the financial year as soon as possible after the end of the relevant period, but at the latest two months thereafter. The issuer shall ensure that the half-yearly financial report remains available to the public for at least five years.

*Documents that shall comprise the half-yearly financial report.....*

2. The half-yearly financial report shall comprise:

- (a) the condensed set of financial statements;
- (b) an interim management report; and

(c) statements made by the persons responsible within the issuer, whose names and functions shall be clearly indicated, to the effect that, to the best of their knowledge, the condensed set of financial statements which has been prepared in accordance with the applicable set of accounting standards gives a true and fair view of the assets, liabilities, financial position and profit or loss of the issuer, or the undertakings included in the consolidation as a whole as required under paragraph 3, and that the interim management report includes a fair review of the information required under paragraph 4.

*Where consolidated accounts are required....*

3. Where the issuer is required to prepare consolidated accounts, the condensed set of financial statements shall be prepared in accordance with the international accounting standard applicable to the interim financial reporting adopted pursuant to the procedure provided for under Article 6 of Regulation (EC) No 1606/2002. Where the issuer is not required to prepare consolidated accounts, the condensed set of financial statements shall at least contain a condensed balance sheet, a condensed profit and loss account and explanatory notes on these accounts. In preparing the condensed balance sheet and the condensed profit and loss account, the issuer shall follow the same principles for recognising and measuring as when preparing annual financial reports.

4. The interim management report shall include at least an indication of important events that have occurred during the first six months of the financial year, and their impact on the condensed set of financial statements, together with a description of the principal risks and uncertainties for the remaining six months of the financial year. For issuers of shares, the interim management report shall also include major related parties transactions.

*Minimum contents of interim management reports...*

5. If the half-yearly financial report has been audited, the audit report shall be reproduced in full. The same shall apply in the case of an auditors' review. If the half-yearly financial report has not been audited or reviewed by auditors, the issuer shall make a statement to that effect in its report.

*Requirements where half-yearly report is, or is not, audited...*

6. The Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures in order to take account of technical developments on financial markets and to ensure the uniform application of paragraphs 1 to 5 of this Article. The Commission shall, in particular:

*The Commission shall  
adopt implementing  
measures concerning  
half-yearly reports*

- (a) specify the technical conditions under which a published half-yearly financial report, including the auditors' review, is to remain available to the public;
- (b) clarify the nature of the auditors' review;
- (c) specify the minimum content of the condensed balance sheet and profit and loss accounts and explanatory notes on these accounts, where they are not prepared in accordance with the international accounting standards adopted pursuant to the procedure provided for under Article 6 of Regulation (EC) No 1606/2002. Where appropriate, the Commission may also adapt the five-year period referred to in paragraph 1.

## Article 6

## Interim management statements

*Requirements for interim management statements: timing and content....*

1. Without prejudice to Article 6 of Directive 2003/6/EC, an issuer whose shares are admitted to trading on a regulated market shall make public a statement by its management during the first six-month period of the financial year and another statement by its management during the second six-month period of the financial year. Such statement shall be made in a period between ten weeks after the beginning and six weeks before the end of the relevant six-month period. It shall contain information covering the period between the beginning of the relevant six-month period and the date of publication of the statement. Such a statement shall provide:

- an explanation of material events and transactions that have taken place during the relevant period and their impact on the financial position of the issuer and its controlled undertakings, and
- a general description of the financial position and performance of the issuer and its controlled undertakings during the relevant period.

*Interim management statements not required where quarterly financial reports published...*

2. Issuers which, under either national legislation or the rules of the regulated market or of their own initiative, publish quarterly financial reports in accordance with such legislation or rules shall not be required to make public statements by the management provided for in paragraph 1.

*Commission to report to the European Parliament and to the Council by 2010 on the transparency of quarterly financial reporting....*

3. The Commission shall provide a report to the European Parliament and the Council by 20 January 2010 on the transparency of quarterly financial reporting and statements by the management of issuers to examine whether the information provided meets the objective of allowing investors to make an informed assessment of the financial position of the issuer. Such a report shall include an impact assessment on areas where the Commission considers proposing amendments to this Article.

## Article 14

*Publication requirements where an issuer acquires or disposes of its own shares...*

1. Where an issuer of shares admitted to trading on a regulated market acquires or disposes of its own shares, either itself or through a person acting in his own name but on the issuer's behalf, the home Member State shall ensure that the issuer makes public the proportion of its own shares as soon as possible, but not later than four trading days following such acquisition or disposal where that proportion reaches, exceeds or falls below the thresholds of 5 % or 10 % of the voting rights. The proportion shall be calculated on the basis of the total number of shares to which voting rights are attached.

*The Commission shall adopt implementing measures concerning the publication of this information*

2. The Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets and to ensure the uniform application of paragraph 1.

## Article 16

*Issuers' obligation to make public any changes in rights attaching to various classes of shares.....*

## Additional information

1. The issuer of shares admitted to trading on a regulated market shall make public without delay any change in the rights attaching to the various classes of shares, including changes in the rights attaching to derivative securities issued by the issuer itself and giving access to the shares of that issuer.

*Issuers' obligation to make public any changes in rights attaching to holders of securities other than shares.....*

2. The issuer of securities, other than shares admitted to trading on a regulated market, shall make public without delay any changes in the rights of holders of securities other than shares, including changes in the terms and conditions of these securities which could indirectly affect those rights, resulting in particular from a change in loan terms or in interest rates.

*Issuers' obligation to make public any new loan issues.....*

3. The issuer of securities admitted to trading on a regulated market shall make public without delay of new loan issues and in particular of any guarantee or security in respect thereof. Without prejudice to Directive 2003/6/EC, this paragraph shall not apply to a public international body of which at least one Member State is member.

## Article 17

Information requirements for issuers whose shares are admitted to trading on a regulated market

*Issuers to ensure equal treatment of all holders of shares....*

1. The issuer of shares admitted to trading on a regulated market shall ensure equal treatment for all holders of shares who are in the same position.

2. The issuer shall ensure that all the facilities and information necessary to enable holders of shares to exercise their rights are available in the home Member State and that the integrity of data is preserved. Shareholders shall not be prevented from exercising their rights by proxy, subject to the law of the country in which the issuer is incorporated. In particular, the issuer shall:

*Issuers' obligations to make available to shareholders information regarding annual meetings, proxy arrangements, etc...*

(a) provide information on the place, time and agenda of meetings, the total number of shares and voting rights and the rights of holders to participate in meetings;

(b) make available a proxy form, on paper or, where applicable, by electronic means, to each person entitled to vote at a shareholders' meeting, together with the notice concerning the meeting or, on request, after an announcement of the meeting;

(c) designate as its agent a financial institution through which shareholders may exercise their financial rights; and

(d) publish notices or distribute circulars concerning the allocation and payment of dividends and the issue of new shares, including information on any arrangements for allotment, subscription, cancellation or conversion.

3. For the purposes of conveying information to shareholders, the home Member State shall allow issuers the use of electronic means, provided such a decision is taken in a general meeting and meets at least the following conditions:

*Member states to allow issuers to use electronic means of conveying information to shareholders.....*

(a) the use of electronic means shall in no way depend upon the location of the seat or residence of the shareholder or, in the cases referred to in Article 10(a) to (h), of the natural persons or legal entities;

(b) identification arrangements shall be put in place so that the shareholders, or the natural persons or legal entities entitled to exercise or to direct the exercise of voting rights, are effectively informed;

(c) shareholders, or in the cases referred to in Article 10(a) to (e) the natural persons or legal entities entitled to acquire, dispose of or exercise voting rights, shall be contacted in writing to request their consent for the use of electronic means for conveying information and, if they do not object within a reasonable period of time, their consent shall be deemed to be given. They shall be able to request, at any time in the future, that information be conveyed in writing, and

(d) any apportionment of the costs entailed in the conveyance of such information by electronic means shall be determined by the issuer in compliance with the principle of equal treatment laid down in paragraph 1.

*The Commission shall adopt implementing measures concerning the above....*

4. The Commission shall, in accordance with the procedure provided for in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets, to take account of developments in information and communication technology and to ensure the uniform application of paragraphs 1, 2 and 3. It shall, in particular, specify the types of financial institution through which a shareholder may exercise the financial rights provided for in paragraph 2(c).

## Article 18

Information requirements for issuers whose debt securities are admitted to trading on a regulated market

*Issuers to ensure equal treatment of all holders of debt securities....*

1. The issuer of debt securities admitted to trading on a regulated market shall ensure that all holders of debt securities ranking pari passu are given equal treatment in respect of all the rights attaching to those debt securities.

*Issuers' obligations to make available to holders of debt securities information regarding annual meetings, proxy arrangements, etc...*

2. The issuer shall ensure that all the facilities and information necessary to enable debt securities holders to exercise their rights are publicly available in the home Member State and that the integrity of data is preserved. Debt securities holders shall not be prevented from exercising their rights by proxy, subject to the law of country in which the issuer is incorporated. In particular, the issuer shall:

(a) publish notices, or distribute circulars, concerning the place, time and agenda of meetings of debt securities holders, the payment of interest, the exercise of any conversion, exchange, subscription or cancellation rights, and repayment, as well as the right of those holders to participate therein;

(b) make available a proxy form on paper or, where applicable, by electronic means, to each person entitled to vote at a meeting of debt securities holders, together with the notice concerning the meeting or, on request, after an announcement of the meeting; and

(c) designate as its agent a financial institution through which debt securities holders may exercise their financial rights.

*In certain circumstances, issuers may hold an annual meeting in another member state...*

3. If only holders of debt securities whose denomination per unit amounts to at least EUR 50000 or, in the case of debt securities denominated in a currency other than Euro whose denomination per unit is, at the date of the issue, equivalent to at least EUR 50000, are to be invited to a meeting, the issuer may choose as venue any Member State, provided that all the facilities and information necessary to enable such holders to exercise their rights are made available in that Member State.

*Member states to allow issuers to use electronic means of conveying information to holders of debt securities.....*

4. For the purposes of conveying information to debt securities holders, the home Member State, or the Member State chosen by the issuer pursuant to paragraph 3, shall allow issuers the use of electronic means, provided such a decision is taken in a general meeting and meets at least the following conditions:

(a) the use of electronic means shall in no way depend upon the location of the seat or residence of the debt security holder or of a proxy representing that holder;

(b) identification arrangements shall be put in place so that debt securities holders are effectively informed;

(c) debt securities holders shall be contacted in writing to request their consent for the use of electronic means for conveying information and if they do not object within a reasonable period of time, their consent shall be deemed to be given. They shall be able to request, at any time in the future, that information be conveyed in writing; and

(d) any apportionment of the costs entailed in the conveyance of information by electronic means shall be determined by the issuer in compliance with the principle of equal treatment laid down in paragraph 1.

5. The Commission shall, in accordance with the procedure provided for in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets, to take account of developments in information and communication technology and to ensure the uniform application of paragraphs 1 to 4. It shall, in particular, specify the types of financial institution through which a debt security holder may exercise the financial rights provided for in paragraph 2(c).

*The Commission shall adopt implementing measures concerning the above....*

## Article 19

## Home Member State control

*Any information disclosed publicly must also be filed with the competent authority*

1. Whenever the issuer, or any person having requested, without the issuer's consent, the admission of its securities to trading on a regulated market, discloses regulated information, it shall at the same time file that information with the competent authority of its home Member State. That competent authority may decide to publish such filed information on its Internet site. Where an issuer proposes to amend its instrument of incorporation or statutes, it shall communicate the draft amendment to the competent authority of the home Member State and to the regulated market to which its securities have been admitted to trading. Such communication shall be effected without delay, but at the latest on the date of calling the general meeting which is to vote on, or be informed of, the amendment.

*Exemptions from above.....*

2. The home Member State may exempt an issuer from the requirement under paragraph 1 in respect of information disclosed in accordance with Article 6 of Directive 2003/6/EC or Article 12(6) of this Directive.

3. Information to be notified to the issuer in accordance with Articles 9, 10, 12 and 13 shall at the same time be filed with the competent authority of the home Member State.

*The Commission shall adopt implementing measures concerning the above....*

4. In order to ensure the uniform application of paragraphs 1, 2 and 3, the Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures. The Commission shall, in particular, specify the procedure in accordance with which an issuer, a holder of shares or other financial instruments, or a person or entity referred to in Article 10, is to file information with the competent authority of the home Member State under paragraphs 1 or 3, respectively, in order to:

- (a) enable filing by electronic means in the home Member State;
- (b) coordinate the filing of the annual financial report referred to in Article 4 of this Directive with the filing of the annual information referred to in Article 10 of Directive 2003/71/EC.

## Article 30

## Transitional provisions

*Transitional provisions:  
exemptions from  
disclosing financial  
statements....*

1. By way of derogation from Article 5(3) of this Directive, the home Member State may exempt from disclosing financial statements in accordance with Regulation (EC) No 1606/2002 issuers referred to in Article 9 of that Regulation for the financial year starting on or after 1 January 2006.

*Transitional provisions:*

2. Notwithstanding Article 12(2), a shareholder shall notify the issuer at the latest two months after the date in Article 31(1) of the proportion of voting rights and capital it holds, in accordance with Articles 9, 10 and 13, with issuers at that date, unless it has already made a notification containing equivalent information before that date. Notwithstanding Article 12(6), an issuer shall in turn disclose the information received in those notifications no later than three months after the date in Article 31(1).

*Transitional provisions:*

3. Where an issuer is incorporated in a third country, the home Member State may exempt such issuer only in respect of those debt securities which have already been admitted to trading on a regulated market in the Community prior to 1 January 2005 from drawing up its financial statements in accordance with Article 4(3) and its management report in accordance with Article 4(5) as long as

(a) the competent authority of the home Member State acknowledges that annual financial statements prepared by issuers from such a third country give a true and fair view of the issuer's assets and liabilities, financial position and results;

(b) the third country where the issuer is incorporated has not made mandatory the application of international accounting standards referred to in Article 2 of Regulation (EC) No 1606/2002; and

(c) the Commission has not taken any decision in accordance with Article 23(4)(ii) as to whether there is an equivalence between the abovementioned accounting standards and

- the accounting standards laid down in the law, regulations or administrative provisions of the third country where the issuer is incorporated, or

- the accounting standards of a third country such an issuer has elected to comply with.

*Transitional provisions:*

4. The home Member State may exempt issuers only in respect of those debt securities which have already been admitted to trading on a regulated market in the Community prior to 1 January 2005 from disclosing half-yearly financial report in accordance with Article 5 for 10 years following 1 January 2005, provided that the home Member State had decided to allow such issuers to benefit from the provisions of Article 27 of Directive 2001/34/EC at the point of admission of those debt securities.

#### 4: Compliance with the UK financial sanctions regime

*The international and UK legislative frameworks for financial sanctions do not prescribe the processes which firms have to adopt to achieve compliance with their legal obligations. This guidance is intended to provide an indication of the types of controls and processes that firms might adopt in order to enable them to comply with sanctions obligations in an effective and proportionate manner. It is not intended to prescribe the manner in which firms must comply with the regime, as much will depend on the nature of the customer base and the business profile of each individual firm. The guidance is intended to assist firms in designing their own processes.*

*Although it is not formal guidance that has been given Ministerial approval, this guidance has been discussed with HM Treasury and reflects their input.*

#### Introduction

##### General

- 4.1 Sanctions can take the form of any of a range of restrictive/coercive measures. They can include arms embargoes, travel bans, asset freezes, reduced diplomatic links, reductions/cessation of any military relationship, flight bans, suspension from international organisations, withdrawal of aid, trade embargoes, restriction on cultural /sporting links and other.
- 4.2 This guidance focuses on financial sanctions and asset freezes, although firms must also be aware of the nature and requirements of other sanctions, especially trade embargoes.
- 4.3 The sanctions regime requires absolute compliance and any person in breach of an obligation under a relevant Statutory Instrument will be guilty of an offence, unless a defence is successfully made out. The nature of the legislation means that firms risk breaching a sanctions obligation as soon as an individual or entity is listed in an EU Regulation, or falls within the remit of a UK Statutory Instrument, the timing of which is outside their control (in contrast to AML approaches, which generally allow firms to set their own timetables on checking and updating customer due diligence details). HMT's intention is ultimately that there is a robust and proportionate response to complying with the sanctions requirements. The penalties for committing an offence are covered in each individual Statutory Instrument. The Terrorist Asset-Freezing etc Act 2010 provides a primary legislative basis for the UK's domestic asset freezing regime .
- 4.4 Notwithstanding the absolute nature of the regime, firms are likely to focus on implementing appropriate systems and controls to identify persons who are subject to financial sanctions, given their assessment of the likelihood of dealing with such persons and associated risk of breaching their obligations. This may involve less immediate or frequent screening and/or being more selective with regard to those who are screened. Firms should note, however, that any provision of funds or financial services etc to, or failure to freeze the assets of, a sanctioned person will expose the firm to the risk of prosecution.

- 4.5 The sanctions regime is absolute and this provides a challenge for compliance. Some firms, for example large firms with millions of customers or which process many millions of transactions every day, will use automated screening systems. Other firms with smaller numbers of customers and transactions may achieve compliance through other processes. Firms must use sanctions checking processes that are proportionate to the nature and size of the firm's business and that in their view are likely to identify all true matches.

*Code for Crown Prosecutors*

- 4.6 If an individual or a firm breaches a financial sanctions prohibition, it will have committed a criminal offence unless a defence is successfully made out. However, in line with the principles set out in the Code for Crown Prosecutors (see Annex 4-IV), prosecution of a firm or individual would only be likely where the prosecuting authorities consider this to be in the public interest, and where they believe that there is enough evidence to provide a realistic prospect of conviction.

***What is the financial sanctions regime?***

*The UK regime*

- 4.7 There is no single Act of Parliament that sets out the UK financial sanctions regime. The UK regime reflects the requirements of various UN Security Council resolutions, and is implemented by way of EU Regulations and UK Statutory Instruments. There are also EU investment ban and trade sanctions regimes that apply in the UK. Annex 4-I summarises these.

*What is a financial sanction?*

- 4.8 Financial sanctions are set out separately in statutory instruments and/or EU Regulations relating to the specific regime. It is generally a criminal offence under the UK implementing legislation directly or indirectly to make funds or economic resources available to or for the benefit of targets on the list unless a licence is obtained from HM Treasury. It is also generally a criminal offence to deal with the funds or economic resources of such targets ("sanctions targets") unless licensed. The terrorism financial sanctions regime also prohibits the provision of financial services to sanctions targets. The prohibitions apply whether dealing directly with targets, or dealing with targets through intermediaries, such as lawyers or accountants. In the case of UK terrorist asset freezing legislation the making available of funds, economic resources and financial services to a person other than the target is only prohibited where to do so would bestow a significant financial benefit on a sanctions target.
- 4.9 In respect of each prohibition, it is a defence for the provider of the funds, economic resources, or where applicable financial services, not to have known or have had reasonable cause to suspect that the prohibition was being breached.

*Penalties*

- 4.10 The penalties for a breach of UK financial sanctions (including breach of EU Regulations containing sanctions, which are applicable in the UK) are set out in the relevant statutory instrument. Any person guilty of an offence is liable on conviction to imprisonment and/or a

fine.

*HM Treasury website*

- 4.11 HM Treasury’s financial sanctions website includes the sanctions legislation applicable in the UK, HM Treasury’s sanctions notifications, Guidance notes and related materials. See [http://www.hm-treasury.gov.uk/fin\\_sanctions\\_index.htm](http://www.hm-treasury.gov.uk/fin_sanctions_index.htm).

*The Consolidated List*

- 4.12 The obligations under the UK financial sanctions regime apply to all firms in the financial sector and not just to banks. In order to assist compliance with the UK regime, the Treasury maintains a ‘consolidated list’ of individuals and entities that are based in the UK or elsewhere that are subject to financial sanctions. The Consolidated List is available at [www.hm-treasury.gov.uk/d/sanctionsconlist.pdf](http://www.hm-treasury.gov.uk/d/sanctionsconlist.pdf).

*UK Investment Ban List*

- 4.13 A list of investment ban targets designated by the European Union under legislation relating to current financial sanctions regimes is available at [www.hm-treasury.gov.uk/d/investmentban.pdf](http://www.hm-treasury.gov.uk/d/investmentban.pdf)
- 4.14 Investment ban targets are not included in the Consolidated List of financial sanctions targets. UK financial firms are prohibited from making new investments in the entities named on the list of investment ban targets. They are not prohibited from making other payments to them or receiving payments from them. This guidance may assist financial institutions in designing processes to prevent new investment in those parties.

*Responsibilities*

- 4.15 Responsibilities for the UK sanctions regime lies with three Government departments:
- (i) HM Treasury
  - (ii) The Foreign and Commonwealth Office (“FCO”), and
  - (iii) The UK Department for Business Innovation and Skills (“BIS”).

The Financial Services Authority also has a role in relation to firms’ systems and controls. Under its financial crime objective, it requires firms, under Principle 3, to have in place appropriate policies and procedures to counter the risk that they might be used to further financial crime. These include adequate systems and controls to comply with the asset freezing regime. Annex 4-II provides a summary of the responsibilities of the UK authorities.

*Overseas jurisdictions*

- 4.16 Where a firm is active in jurisdictions outside the UK, it may be required to comply with the requirements of the sanctions regimes in other jurisdictions. Some jurisdictions’ requirements may also apply without a firm having an actual presence in that jurisdiction.
- 4.17 Firms will need to understand which sanctions regimes impact on which parts of their business and ensure they correctly comply with applicable sanctions while not incorrectly

applying regimes of other jurisdictions to UK business. Annex 4-IV contains links to some useful websites.

### ***Approach, Procedures and Training***

#### *Approach – what does an asset freeze do?*

- 4.18 An asset freeze prohibits dealings with the funds or economic resources of a sanctions target. It also prohibits making funds or economic resources (and in relation to those designated under the terrorism regime, financial services) available, directly or indirectly, to or (in the case of those designated under the terrorism regime) for the benefit of sanctions targets. Firms should therefore implement appropriate means of control to prevent breaches of prohibitions. It is a criminal offence for a firm to breach a sanctions prohibition.
- 4.19 In order to reduce the likelihood of breaching obligations under financial sanctions regimes, firms are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with sanctions targets and where meaningful information on their clients, counterparties and transactions is held. Within this approach, firms are likely to focus their prevention and detection procedures on direct customer relationships, and on transactions, having appropriate regard to other parties involved. However, firms cannot ignore “low risk” areas and must ensure that systems and controls also pay attention to areas where dealings with a sanctions target are unlikely, but possible.

#### *Policy and senior management responsibilities*

- 4.20 Firms should have a sanctions policy that is informed by a thorough understanding of legal requirements applied to an assessment of the risks in their firm. Senior management and/or the Board of a firm should understand the firm’s obligations and take responsibility for the firm’s sanctions compliance policies and procedures.

#### *Approach tailored to business model*

- 4.21 Firms should take an approach which is appropriate for their business model, when assessing where and how their business is most likely to encounter sanctioned parties, and to focus resources and tailor systems and controls accordingly.
- 4.22 Firms, particularly those with many different client types, product types and/or geographical markets, should consider carrying out an assessment in order to be able to understand which parts of their business may carry a greater likelihood of breaching the requirements of economic or terrorist-related sanctions. Any assessment may usefully include a high level assessment of the firm’s view of its business profile in specific business areas, and information on periodic CDD and other checks relating to those areas.
- 4.23 An assessment should start with identification and assessment of the issues that have to be managed. A firm should develop its approach in the context of how it might most likely be involved in breaching economic and country-related sanctions. A firm may take into account a range of factors when conducting its assessment, including:
- Its customer, product and activity profiles
  - Its distribution channels
  - The complexity and volume of its transactions

- Its processes and systems
- Its operating environment
- The screening processes of other parties
- The geographic risk of where it does business
- The sanctions regulations of relevant countries.

*Documenting the assessment*

- 4.24 Firms should document the assessment and approach adopted on the basis of that assessment. Firms should also identify where a decision is taken to adopt a different approach where this may go beyond a particular requirement.

*Firms' activities outside the UK*

- 4.25 UK sanctions legislation typically applies to UK persons and persons in the UK, including bodies incorporated or constituted under UK law. Where firms operate in a number of countries or territories, a consistent group wide 'umbrella' policy should be established, which can assist local business units in ensuring that their local procedures meet minimum group standards. Firms will also need to take account of any particular local, legal requirements. Foreign subsidiaries of UK firms that have a separate legal personality outside the UK (as distinct from branches) would not be covered by UK sanctions law, but by the law of the jurisdiction in which they are based.

*Procedures*

- 4.26 Firms should ensure that appropriate policies and procedures are in place across the organisation. A firm's procedures should be appropriate to its business, and readily accessible and well understood by all relevant staff. Senior management must understand and stress the importance of understanding and complying with the firm's policies and procedures.
- 4.27 Firms should ensure that their procedures remain up to date and fit for purpose in a changing environment. Firms may use internal review, other appropriate functions or external review to achieve this.
- 4.28 Firms should ensure that they communicate in a timely manner to relevant staff changes to the sanctions requirements, including any internal changes to systems, procedures and controls.
- 4.29 Firms should adequately monitor their systems processes and controls to support full compliance with sanctions requirements.

*Staff Training*

- 4.30 A firm should have staff training programmes commensurate with its business and risk profile. Firms should consider implementing arrangements for:
- providing material containing the firm's financial sanctions policies and procedures which is readily available and simple to understand;
  - providing training that is appropriately tailored for different groups of staff to reflect the

likelihood of different degrees of staff involvement with sanctions issues, including what to do in the event of a reportable match;

- providing refresher training, delivered at appropriate intervals.

#### *Circumvention*

4.31 Firms' policies and procedures should include provisions to prohibit and detect attempts to circumvent sanctions, by, for example:

- omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by other firms in the payment process, or
- structuring transactions with the purpose of concealing the involvement of a sanctioned party.

Employment contracts should make any such attempt a serious disciplinary offence.

#### *Screening of customers and transactions*

4.32 Firms should have processes to manage the risk of conducting business with or on behalf of individuals and entities on the Consolidated List (which includes all the names of sanctioned persons and entities under UN and EU sanctions regimes which have effect in the UK). Firms should consider screening their customers on a periodic basis, and certain transaction data. The Consolidated List is available at [www.hm-treasury.gov.uk/d/sanctionsconlist.pdf](http://www.hm-treasury.gov.uk/d/sanctionsconlist.pdf)

#### *Taking a tailored approach*

4.33 As already noted, it is for individual firms to assess how best to comply with the financial sanctions legislation within the context of their business activities and profile. The prohibitions in the legislation extend beyond payments made directly to sanctions targets, i.e., payments which are made indirectly to, or which are made to others for the benefit of, sanctions targets are within the scope of the legislation.

4.34 An "indirect payment" is one that is made to someone acting on behalf of the sanctions target. In contrast, the prohibition on making payments to others for the benefit of a sanctions target is intended to prevent payments being made to third parties to satisfy an obligation of that person.

4.35 As explained in paragraphs 4.18ff, firms should adopt an approach informed by the profile of their business model and client base. Firms are likely to focus their screening processes on areas of their business that carry a greater likelihood of involvement with sanctions targets, or their agents, although as outlined earlier, low risk areas cannot be ignored.

#### *Record of screening policy*

4.36 Firms should keep a written record of their screening policy and be able to justify the timescales and frequency of screening, resolution of screening matches and regulatory reporting if required.

#### *Review of processes*

4.37 Firms should review, and update their processes periodically, so that they remain appropriate

for their needs and ensure that any internal guidance is updated to reflect major changes to the sanctions regime, such as the addition of a new jurisdiction or regime.

#### *Elements of screening process*

- 4.38 The scope and complexity of the screening process will be influenced by the firm's business activities, and according to the profile of the firm. An effective screening process should include the following elements:
- it should flag up potential name matches against the Consolidated List and names against which measures have been issued under the Counter-Terrorism Act
  - potential matches should be reviewed by appropriately trained staff
  - where matches are confirmed as true, appropriate action should be taken to freeze the account
  - true matches should be reported as soon as is practicable to the Asset Freezing Unit at HM Treasury (see paragraphs 4.62ff for the reporting of matches) and
  - it should maintain an audit trail of actions around potential and true matches.

#### *Screening software*

- 4.39 Many firms use automated customer screening software provided by a commercial provider; other firms rely on manual screening. Firms may consider whether and what type of screening software to use in line with the nature, size and risk profile of their business. A key element of a screening system is that it will flag potential matches clearly and prominently. Firms should document the reasons for choosing whichever screening method they decide to use.
- 4.40 Where commercially available automated screening software is implemented, firms should understand its capabilities and limits, and make sure it is tailored to their business requirements, data requirements and risk profile. Firms should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used, firms should be satisfied that they have adequate contingency arrangements should the software fail and should periodically check the software is working as they expect it to.

#### *Legacy systems*

- 4.41 Firms should be alert to any operational issues which may arise from having the risk of customer or transaction data in legacy systems.

#### *'Fuzzy matching'*

- 4.42 It is important to consider "fuzzy matching", as names might be missed if only exact matches are screened. "Fuzzy matching" describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data - whether in official lists or in firms' internal records - is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process.
- 4.43 Where a firm uses a screening system which has a fuzzy matching capability, it should

ensure that the fuzzy matching process is calibrated as appropriate in line with the risk profile of their business.

- 4.44 Application of a fuzzy matching process to a screening system will result in the generation of an increased number of apparent matches which have to be checked. The generation and resolution of an undue number of false positives may have a negative impact on the efficacy of the resolution process. Firms should therefore consider the level of appropriate human intervention to assess which results may be false positives.

*Use of false personal information*

- 4.45 Sanctioned parties are known to use false personal information to try and evade detection of their illicit activities. Typical approaches are to use name variations, e.g., name reversal and removing numbers from the names of entities, etc. For this reason, many firms use screening tools which screen using several protocols – e.g., name reversal, number removal, number replaced by word, etc.

*Outsourcing and reliance*

- 4.46 A firm may outsource screening and/or other financial sanctions compliance processes to a contractor, but will remain fully responsible for discharging all of its regulatory obligations. Firms may therefore consider putting in place an appropriate Service Level Agreement with contractors and should satisfy themselves that the outsourced party is providing an effective service.
- 4.47 There is no “reliance” provision in the UK financial sanctions regime. When screening customers and related parties that are new to the firm but who are or were already clients of another FSA-authorised firm, firms might choose to consider this in their assessment when determining their screening policy. However, it should not be assumed that such clients have already been screened.

*Timing of screening*

- 4.48 All customers should be screened during the establishment of a business relationship or as soon as possible after the business relationship has commenced. Firms should be aware of the risks associated with screening customers after a business relationship has been established and/or services have been provided i.e., that they may transact with a sanctioned party in breach of sanctions prohibitions. Firms must be aware of the absolute restrictions embedded in the financial sanctions regime. Where there is any delay in screening, firms face a risk of breaching the legislation.
- 4.49 For low-risk business a firm might choose post-event screening, provided the nature of the business allows the firm to prevent movement or withdrawal of the asset(s) concerned until the sanction check has been completed.
- 4.50 In accordance with a firm’s business profile, consideration should be given to how often customer re-screening should be carried out. Some firms carry out regular periodic systems-based screening of their entire customer data. Others develop a programme to re-screen for changes to their customer list and changes to the Consolidated List. Firms should ensure that they have adequate arrangements to screen when changes are made to the Consolidated

List.

*Screening of associated parties*

- 4.51 The sanctions prohibitions also apply to both indirect payments to and payments for the benefit of sanctions targets. Where practicable, screening should cover any other related parties, for example beneficial owners (including trustees, or company directors), that are identified by the firm in question as requiring verification under its risk-based approach to customer due diligence. A firm's judgement in these matters will need to be consistent with its approach for AML purposes, and whether or not full identity details are collected.
- 4.52 Firms may choose not to undertake financial sanctions checks in respect of particular related parties associated with an investment if its assessment considers such checks would be disproportionate in particular cases. Firms should be aware, however, that this will increase the risk of sanctions legislation being breached. Firms may be liable to prosecution in respect of any such breaches.

*Dormant accounts*

- 4.53 Firms may wish to consider whether dormant accounts should be screened, and if so how and when they should be screened. This decision is likely to reflect the firm's risk policy, and the availability or otherwise of dormant account data on a system that is able to be screened.

*Transaction screening*

- 4.54 Firms should monitor higher-risk payment instructions to assist in preventing a breach of the prohibitions. Transactions screening involves screening of payment information to identify potential sanction targets.
- 4.55 Transaction screening should take place on a real-time payment basis, i.e., the screening or filtering of relevant payment instructions should be carried out before the transaction is executed.
- 4.56 Firms will approach transaction screening in line with their assessment of their business risks. Firms are likely to focus on screening international transactions where there is adequate information on third parties, and parties to trade finance deals plus walk-in customers wishing to send payments both within and outside the UK. Firms that operate client money accounts or provide safe custody services are likely to focus on third party payments and asset transfers.
- 4.57 Banks will wish to consider screening both data in the payment and relevant advice messages (e.g., MT103, MT910, MT202 etc) and for intermediary banks data in the cover payments e.g., MT202COV.
- 4.58 Factors that firms may consider when determining which transactions should be screened include:
- whether automated screening is possible
  - industry best practice
  - international / domestic connections

- adequate information to ascertain whether it is a potential match
- materiality of transaction
- the nature of the client's business
- analysis of historical sanction matches

- 4.59 When funds are received electronically by a financial firm as payee (i.e., not a Payment Service Provider in the transaction – see Part I, paragraph 5.2.11), the name of the payer will typically not be passed on by the PSP to the payee. The payee firm is not expected to screen the payer nor to screen the incoming payment, unless there is reason to believe the payer is not their customer.
- 4.60 When funds are received electronically by a Payee Payment Services Provider from within the EU, the payer's name and address may not be included in the transfer (as it is not required in the relevant legislation – see section 1: *Transparency in electronic payments (wire transfers)*, paragraph 1.14). The PSP may need to consider whether to request additional information in order to meet its sanctions obligations.

*Audit trail and record keeping*

- 4.61 Whether firms screen using automated systems or manually, an audit trail should be maintained for a period of no less than five years. This should record all relevant information to a likely match, how it was resolved and the rationale applied. Firms should ensure that their processes are kept under review, and remain up to date, and appropriate for the needs of the institution.

**Reporting matches and breaches of the regime**

*Assessing possible matches*

- 4.62 Firms may often find it difficult to determine if there are true matches i.e., they involve a sanctioned party. Potential matches should be investigated and reviewed as appropriate to confirm if they are true matches. The majority of matches are likely to be “false positives” and after this is confirmed there will be no need for further review. Sophisticated screening software permits adjustment of screening rules, so as to prevent repetition of specific false matches.
- 4.63 True matches are where a firm has no doubt that the account held is that of a target of the financial sanctions regime. It is also possible to have a potential match where a name of a customer may appear to match the name of a target included on HM Treasury's Consolidated List. Firms should seek to obtain sufficient information to enable them to confirm or eliminate a partial match. This process should be documented in writing.

*What is a false positive?*

- 4.64 A “false positive” is the identification of an apparent match to a record on the Consolidated List (or a party against which measures have been issued under the Counter-Terrorism Act) which is assessed on investigation not to relate to a sanctions target or entity.
- 4.65 Time constraints are also particularly relevant in the context of payments. Firms may make further enquiry either from the counter-party bank or from their client or both, so as to assist

in determining whether the match is a true match. Firms should seek sufficient information to enable them to confirm or eliminate a potential match. This process should be documented in writing. For cases that are assessed to be not a true match, firms should ensure that there is a clear rationale for deciding that an apparent match is a false positive and that this rationale can be demonstrated.

- 4.66 Every potential match of a customer account should be checked, and if appropriate investigated. This process should be documented in writing. Firms are advised to keep an appropriate audit trail about every likely match. This is likely to include a record of who made the decision and on what grounds.

*Reporting to HM Treasury*

- 4.67 Where firms believe that they hold funds or assets for a sanctioned party, this must always be reported to the Asset Freezing Unit at HM Treasury as soon as practicable – see Annex 4-II. Firms must ensure that they have clear internal and external reporting processes for reporting matches to HM Treasury as soon as practicable and that individuals within the firm dealing with matters in relation to which a report has been made to HM Treasury understand their obligations.

*What information to report?*

- 4.68 Firms are generally required to report the following information:
- the information or other matter on which the knowledge or belief is based;
  - any information held by the financial institution about the sanctions target by which the person can be identified; and
  - the nature and amount or quantity of any funds or economic resources held by the financial institution for the sanctions target.

*Legislative reporting requirements*

- 4.69 Firms should comply with the specific requirements of the applicable legislation, which may be contained in a UK Statutory Instrument or in an EU Regulation (available from the HM Treasury sanctions website) as regards their obligations in dealing with sanctioned parties. As legislation relating to different sanctioned parties may vary, the detail of the relevant legislation covering the asset freeze should be examined. Firms may also seek advice from HM Treasury's Asset Freezing Unit on the action required, including where serious practical difficulties arise with regard to compliance.
- 4.70 In the case of sanctions contained in UK Statutory Instruments, HM Treasury may (depending on the applicable Statutory Instrument) in addition ask any UK person (as defined in the relevant Statutory Instrument) to provide information that they may reasonably require for the purpose of monitoring compliance and detecting evasion of the sanctions regime [see for example the Terrorism (United Nations Measures) Order 2009 Schedule Part I (4)].

*Contacting customer's branch*

- 4.71 Where a customer's account has been frozen, firms may need to contact the customer's local branch or appropriate business area informing them of the asset freeze.

*Notifying customer of asset freeze - does "tipping off" apply?*

- 4.72 Firms will usually wish to consider notifying the customer or parties to a relevant transaction what action has been taken and the reason for that action. Informing the customer or third parties of a party's sanctioned status is not prohibited (unless the person's designation has been made known to only a restricted number of firms on HM Treasury's restricted access website and HM Treasury has specified that the designation is confidential information and not to be disclosed further). It is not of itself a 'tipping off' offence under the Proceeds of Crime Act 2002 ("POCA"), as the fact that a party is sanctioned is public information (unless it is specified to be confidential in the circumstances described above). By contrast, if the firm has filed a Suspicious Activity Report ("SAR") under POCA or the Terrorism Act 2000, ("Terrorism Act"), disclosing that fact (i.e., the fact of filing of the SAR) will be a 'tipping off' offence.
- 4.73 Firms may choose to advise the customer/parties to a transaction that concerns as to the effect of the financial sanction may be raised with the Asset Freezing Unit at HM Treasury.

*Does a SAR have to be filed?*

- 4.74 Holding an account for a sanctioned party or rejecting or processing a transaction (whether or not in breach of financial sanctions prohibitions) which involves a sanctioned party, is not in itself grounds for filing a SAR under either POCA or the Terrorism Act.
- 4.75 However, should a suspicion of crime or terrorism arise, firms should consider their obligations under the legislation and whether they should submit a SAR.

*Reporting to the FSA*

- 4.76 There is no formal legal requirement to report a true match other than to the Asset Freezing Unit at HM Treasury.
- 4.77 The FSA has indicated that it regards breaches (not true matches) of financial sanctions to be a matter that would be appropriate for firms to report to the FSA via their usual points of contact. This disclosure should be consistent with the FSA's Principle 11 which requires a firm to "deal with its regulators in an open and co-operative way" and to "disclose to the FSA anything relating to the firm of which the FSA would reasonably expect notice". Firms with a dedicated FSA relationship manager may wish to discuss the practicalities of this as part of their usual supervisory dialogue.

*Review customer relationship*

- 4.78 Firms may wish to review their relationship with a customer confirmed as a true sanctions match.

*Breaches of Statutory Instruments*

- 4.79 HM Treasury must be informed as soon as practicable where a firm knows or suspects that an offence under any one of the various sanctions has been committed either by itself or by a sanctions target. Failure to do so constitutes an offence.

## ANNEX 4-I

<b>Summary of relevant legislation</b>
--

*Note: This summary focuses on legislation relating to terrorism and terrorist financing. Not all country-based regimes are, however, in place for this purpose; some are more human rights based.*

**United Nations**

UNSCR 1373 (2001) The UN Security Council has passed UNSCR 1373 (2001) which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UN Security Council Resolutions regarding terrorism can be found at [www.un.org/Docs/sc/committees/1373/](http://www.un.org/Docs/sc/committees/1373/)

UNSCR 1267 (1999) The UN has published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama Bin Laden, Al-Qa'ida, and the Taliban under UNSCR 1267 (1999), 1390 (2002) and 1617 (2005). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

**European Union**

EC Regulation 2580/2001 as amended The EU directly implements all UN financial sanctions, including financial sanctions against terrorists, through binding and directly applicable EU Regulations. The EU implemented UNSCR 1373 through the adoption of Regulation EC 2580/2001 (as amended). This Regulation introduces an obligation in Community law to freeze all funds and economic resources belonging to named persons and entities, and not to make any funds, economic resources or financial services available, directly or indirectly, to those listed.

EC Regulation 881/2002 (as amended) UNSCR 1267 and its successor resolutions are implemented at EU level by Regulation EC 881/2002 (as amended).

The texts of EC Regulations referred to and the lists of persons targeted, are available at [http://ec.europa.eu/external\\_relations/cfsp/sanctions/docs/measures\\_en.pdf](http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf)

**UK legislation**

The UK has implemented its obligations under UNSCR 1373 under the Terrorist Asset-Freezing Act 2010 (which replaced the Terrorism (United Nations Measures) Orders of 2001, 2006 and 2009). The 2001 and 2006 Orders had been replaced and revoked by the 2009 Order save that directions designating persons under article 4 of the 2001 and 2006 Orders which remained in force on the date of the 2009 Order came into force continued to

apply and the provisions of the 2001 and 2006 Orders continued to apply to such directions.

UNSCR 1267 and its successor resolutions are implemented in the UK by EC Regulation 881/2002 (as amended). The Al-Qa'ida and Taliban (Asset-Freezing) Regulations 2010 provide for penalties of Regulation 881/2002 and, amongst other things, reporting obligations on financial institutions.

Acting under the Terrorist Asset-Freezing etc Act 2010, where HM Treasury has reasonable grounds for suspecting that the person is a person who commits, attempts to commit, facilitates or participates in the commission of acts of terrorism, and it considers the designation necessary for the purposes of protecting members of the public from a risk of terrorism, it can designate that person for the purposes of the Order. This might result in the addition of a name to the HM Treasury list that might not appear on the equivalent UN or EU lists.

A number of organisations have been proscribed under UK anti-terrorism legislation. Where such organisations are also subject to financial sanctions (an asset freeze), they are included on the Consolidated List maintained by HM Treasury.

### ***Regimes currently in place***

[A list of the terrorism and terrorist financing regimes currently in place can be found on the HM Treasury website at:   
http://www.hm-treasury.gov.uk/fin\\_sanctions\\_currentindex.htm](http://www.hm-treasury.gov.uk/fin_sanctions_currentindex.htm)

### ***Other regimes***

The Department for Business, Innovation and Skills is the UK department responsible for trade sanctions.

Certain trade sanctions regimes, such as those involving an arms embargo, also include measures that place restrictions on the provision of financial assistance related to specific activities, such as military activities.

Below are details of those trade sanctions regimes in effect in the UK, which include restrictions on the provision of finance directly to the prohibited trade activities:

#### Lebanon

The Counter  
Terrorism Act 2008

Schedule 7 to the CTA gives power to HM Treasury to issue directions to firms in the financial sector. The kinds of requirement that may be imposed by a direction under these powers relate to

customer due diligence;  
ongoing monitoring;  
systematic reporting ;  
limiting or ceasing business.

**Deleted:** Terrorism and terrorist financing¶  
¶  
Al Qaeda & Taliban¶  
Belarus¶  
Burma/Myanmar¶  
Democratic Republic of Congo¶  
Eritrea¶  
Federal Republic of Yugoslavia and Serbia¶  
[International Criminal Tribunal for The Former Yugoslavia](#)¶  
Iran¶  
Iraq¶  
Ivory Coast¶  
Lebanon and Syria¶  
Liberia¶  
North Korea (Democratic People's Republic of Korea)¶  
Republic of Guinea¶  
Somalia¶  
Sudan¶  
Zimbabwe¶

The requirements to carry out CDD measures and ongoing monitoring build on the similar obligation under the Money Laundering Regulations. The requirements for systematic reporting and limiting or ceasing business are new.

HM Treasury may give a direction **if one or more** of the following conditions is met in relation to a non-EEA country:

- that the Financial Action Task Force has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities being carried on
  - (a) in the country,
  - (b) by the government of the country, or
  - (c) by persons resident or incorporated in the country.
- that the Treasury reasonably believe that there is a risk that terrorist financing or money laundering activities are being carried on
  - (a) in the country,
  - (b) by the government of the country, or
  - (c) by persons resident or incorporated in the country,

**and** that this poses a significant risk to the national interests of the UK.
- that the Treasury reasonably believe that
  - (a) the development or production of nuclear, radiological, biological or chemical weapons in the country, or
  - (b) the doing in the country of anything that facilitates the development or production of any such weapons,

poses a significant risk to the national interests of the UK.

### Summary of responsibilities for the UK regime

Responsibilities lie with three Government departments and the Financial Services Authority also has a role:

1. The Foreign and Commonwealth Office (“FCO”) has responsibility for negotiating in the UN and in the EU on sanctions
2. The Department for Business Innovation and Skills (“BIS”) has responsibility for trade sanctions.
3. HM Treasury has responsibility for administering sanctions in the UK, compliance and issuing exemptions to prohibitions by way of licence.
4. The Financial Services Authority (“FSA”) has responsibility for ensuring that financial services firms have adequate systems and controls for compliance with the UK financial sanctions requirements.

#### **The FCO**

The FCO has responsibility for UK policy in relation to the scope and content of the sanctions regime. The FCO also has responsibility for representing and negotiating the UK’s position with respect to the terms of financial sanctions related United Nations Security Council resolutions and European Union Regulations. UNSCRs provide the basis on which the legal sanctions framework is constructed, and EC Regulations give effect to UN obligations in the EU, including in the UK.

The EU can also impose autonomous sanctions within the framework of the Common Foreign and Security Policy.

The FCO maintains a list of current restrictions and information on the countries that are under export controls and sanctions: see [www.fco.gov.uk/resources/en/word/doc2/sanctions-regimes](http://www.fco.gov.uk/resources/en/word/doc2/sanctions-regimes)

#### **BIS**

BIS has responsibility for trade sanctions, setting export controls and administering the FCO list of about 50 countries subject to trade measures. Trade sanctions, such as embargoes on making military hardware or know-how available to certain named countries of jurisdictions, can be imposed by governments or other international authorities, and these can have financial implications. Firms which operate internationally should be aware of such sanctions, and should consider whether these affect their operations; if so, they should decide whether they have any implications for the firm’s procedures. Further information and links to lists of affected countries can be found at [www.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index](http://www.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index)

BIS also has specific responsibility for implementing United Nations Security Council Resolutions on weapons of mass destruction. Within BIS the Export Control Organisation (“ECO”) has responsibility for legislating, assessing and issuing export licences for specific categories of “controlled” goods. This encompasses a wide range of items including so-called dual-use goods,

torture goods, radioactive sources, as well as military items. A licence may be required depending on various factors including the nature of the items exported and any sanctions in force on the export destination.

### **HM Treasury**

HM Treasury is the lead UK Government department on financial sanctions. The key objective of HM Treasury's Asset Freezing Unit (AFU) is to ensure a proactive and effective UK asset freezing regime in partnership with stakeholders. The AFU has four branches, covering Counter-terrorism, International, Licensing and Compliance.

### **The FSA**

The FSA Handbook, in particular Principle 3 and SYSC 6.1.1, places specific responsibilities on firms regarding financial crime prevention. Authorised firms are therefore subject to regulatory requirements relating to the UK's financial sanctions regime.

The following are the specific requirements:

Principle 3: Management and control

“A firm must take reasonable care to establish and control its affairs responsibly and effectively with adequate risk management systems” and

SYSC 6.1.1

“A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime. [Note: article 13(2) of MiFID.]”

### **Application in law**

Sanctions apply in UK law through both EC Regulations and Statutory Instruments (which have been used as the UK's enabling legislation for the application of UN financial sanctions). With regard to EC Regulations, there is direct applicability in EU Member States, so that entities incorporated or constituted under EU law, and persons and entities doing business in the EU (including non-EU nationals) are subject to their provisions. Statutory Instruments apply to any person in the UK and any British citizen, and any body incorporated or constituted under law of any part of the UK (but not subsidiaries operating outside the UK with no UK legal personality). Annex 4-I provides details of international, EU and UK legislation relevant to financial sanctions and asset freezing.

Each Statutory Instrument is unique in terms of detail, restrictions, exceptions, prohibitions the penalties for non-compliance and information requirements.

### **Who must comply with financial sanctions in the UK?**

The relevant Statutory Instruments generally apply to any person in the UK, to any person elsewhere who is a British citizen or subject, and to any body incorporated or constituted under the

law of any part of the UK, although the exact wording may differ from one Statutory Instrument to another. The UK statutory instruments do not apply to subsidiaries operating wholly outside the UK and which do not have legal personality under UK law.

EU Regulations imposing and/or implementing sanctions are part of Community law, are directly applicable and have direct effect in the Member States. The measures apply to nationals of Member States, as well as persons and entities doing business in the EU, including nationals of non-EU countries.

**Is it an offence to make funds available to a target of financial sanctions legislation?**

This is covered specifically in each relevant Statutory Instrument and EU Regulation. In general terms, any person to whom the relevant legislation applies who, except under the authority of a licence granted by HM Treasury under the relevant legislation makes any funds, economic resources or, in some circumstances, financial (or related) services available directly or indirectly to or for the benefit of persons listed under the relevant Statutory Instrument or EU Regulation is guilty of an offence.

**What are the penalties for committing an offence under the legislation?**

These are covered specifically in each relevant Statutory Instrument. However, in general terms, any person guilty of an offence under the relevant Statutory Instrument is liable on conviction to imprisonment and/or a fine. The maximum term of imprisonment is currently seven years or two years in the case Statutory Instruments providing penalties for breaches of EU Regulations.

Where any body corporate is guilty of an offence under the relevant Statutory Instrument, and that offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, that person as well as the body corporate is guilty of that offence and is liable to be proceeded against and punished accordingly.

**Subscribing to HM Treasury notification service**

The Asset Freezing Unit offers a free subscription facility for notification by e-mail when a Financial Sanctions-related release is published on this website and the consolidated list of targets is updated. In order to subscribe, an email should be sent from the email address to be subscribed to [AFUsubscribe@hmtreasury.gsi.gov.uk](mailto:AFUsubscribe@hmtreasury.gsi.gov.uk) with the words **SUBSCRIBE SANCTIONS** in the subject field, and providing your name, company name, address and telephone number as appropriate.

**The BBA alert service**

The BBA provides an additional alert service by notifying its members and drawing their attention to amendments published by HM Treasury. The alert service is provided to all BBA member banks and principal contacts.

**International requirements**

Firms active in non-UK jurisdictions will wish to be aware of the sanctions requirements in each and every country where they operate.

## Summary of Licensing Regime

### What is a licence?

A licence is a written authorisation from HM Treasury to allow an activity which would otherwise be prohibited by financial sanctions legislation. The obligations and responsibilities attached to a licence are generally imposed on a sanctions target, but a licence may be issued to a relevant financial institution in order to allow such institution to engage in an activity, such as dealing with funds belonging to a sanctions target, which would otherwise be prohibited. A licence may include associated reporting requirements or other conditions on a financial institution, and these will be made clear in the terms of an individual licence.

Applications to release funds from frozen accounts, or to make funds, economic resources or financial services available to or for the benefit of a sanctions target must be made in writing to the Asset Freezing Unit, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ, or emailed to [assetfreezingunit@hmtreasury.x.gsi.gov.uk](mailto:assetfreezingunit@hmtreasury.x.gsi.gov.uk).

HM Treasury will normally provide guidance letters when issuing licences to banks. Such guidance will specify the purpose for which the licence is being issued, together with any specific obligations on financial institutions including any monitoring requirements.

### Operation of frozen accounts under a licence

HM Treasury does not instruct financial institutions on how they should operate frozen accounts that are licensed to permit specific transactions to take place. Some financial institutions operated such accounts by blocking all electronic functionality, or permitting only specified standing orders/direct debits. Other financial institutions allow the accounts to be operated without restrictions, but apply specific monitoring. Where accounts are operated openly, financial institutions must ensure that there is sufficient monitoring to satisfy themselves that any breaches by a sanctions target, for example withdrawals in excess of a cash limit stated in the licence, are identified as soon as possible and reported to HM Treasury.

There are primarily four different models by which frozen accounts are operated:

- i. frozen accounts of sanctions targets subject to a licence are run as standard accounts with cash cards and full electronic functionality. Monitoring is in place on such accounts to ensure any unauthorised activity by the sanctions target is detected and communicated to HM Treasury without delay.
- ii. the original account is frozen and a new account is opened that benefits or other licensed income can be paid into. The sanctions target has no access to funds in the original frozen account. Again, monitoring is in place on such account to detect any unauthorised activity.
- iii. access to a cash card is withdrawn. However, the sanctions target is permitted to set up payments, e.g., for rent and utilities, by standing order or direct debit. Remaining funds required (up to a limit specified in the licence) must be withdrawn in person at the

branch counter.

iv. the account is blocked to remove all electronic functionality, and the sanctions target must withdraw cash over the branch counter – there may be a limit on the amount of cash that can be withdrawn, depending on the terms of the licence.

Depending on the model of account operation adopted, there is a balance between ensuring that sufficient controls are in place on such accounts and ensuring that the impact of the asset freezing regime on the individual is not disproportionate.

In respect of the insurance industry, especially general insurance, there may be instances where legitimate third party claims may arise. In such circumstances any payments or services provided may require a licence or amending the current licence. In all instances the advice of HM Treasury should be obtained before any payment is made.

Even where no obligations on a bank are specified in a licence, there are relevant obligations contained in the legislation itself. Part 4 of the 2009 Terrorism Order imposes certain reporting obligations on financial institutions in relation to offences committed under Article 8 and Part 3 of the Order. Where a financial institution is aware of breaches of the asset freeze by a sanctions target, there is a requirement to inform the Asset Freezing Unit as soon as it is practicable to do so. One example is that in a circumstance where a bank is aware, through monitoring of an account, that a sanctions target is in breach of their licence conditions, e.g., through withdrawing more cash than they are permitted, the bank is required by the legislation to inform HM Treasury of the sanctions target's breach as soon as is practicable.

Guidance on, and examples of, General Licences is available on the HM Treasury website at [http://www.hm-treasury.gov.uk/fin\\_sanctions\\_general\\_licences.htm](http://www.hm-treasury.gov.uk/fin_sanctions_general_licences.htm).

**Useful sources of information**

UN Security Council: [www.un.org/Docs/sc/committees/INTRO.htm](http://www.un.org/Docs/sc/committees/INTRO.htm).

HM Treasury: [http://www.hm-treasury.gov.uk/fin\\_sanctions\\_index.htm](http://www.hm-treasury.gov.uk/fin_sanctions_index.htm)

FCO: <http://www.fco.gov.uk/en/global-issues/counter-terrorism/>

Code for Crown Prosecutors: [www.cps.gov.uk/publications/docs/code2004english.pdf](http://www.cps.gov.uk/publications/docs/code2004english.pdf)

Home Office: [www.homeoffice.gov.uk/security/terrorism-and-the-law](http://www.homeoffice.gov.uk/security/terrorism-and-the-law)

SOCA: [www.soca.gov.uk](http://www.soca.gov.uk)

European Commission: [http://ec.europa.eu/external\\_relations/cfsp/sanctions/list/consol-list.htm](http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm)

FSA report on firms' compliance with UK sanctions requirements:  
[www.fsa.gov.uk/pubs/other/Sanctions%20Final%20Report.pdf](http://www.fsa.gov.uk/pubs/other/Sanctions%20Final%20Report.pdf)

Department for Business Innovation and Skills (formerly Department of Trade and Industry):  
<http://www.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index.ht>

US Treasury: <http://www.ustreas.gov/offices/enforcement/ofac/programs/>

OFAC: <http://www.treas.gov/offices/enforcement/ofac/>

FATF: [www.fatf-gafi.org/](http://www.fatf-gafi.org/)

Wolfsberg Group: <http://www.wolfsberg-principles.com/>

## 5: Directions under the Counter-Terrorism Act 2008, Schedule 7

### *HM Treasury power to issue directions*

- |                      |     |  |
|----------------------|-----|--|
| CTA 2008 c 28        | 5.1 | The CTA gained royal assent on 26 November 2008 and came into force on that date. The UK Government has deemed it a necessary further tool in the range of legislation to address the risks from money laundering, terrorist financing and the proliferation of nuclear, radiological, biological or chemical weapons.   |
| CTA Sch 7, para 9(4) | 5.2 | Schedule 7 to the CTA gave new powers to HM Treasury to issue directions to firms in the financial sector. The kinds of requirement that may be imposed by a direction under these powers relate to <ul style="list-style-type: none"> <li>○ customer due diligence (see paragraph 5.21);</li> <li>○ ongoing monitoring (see paragraph 5.31);</li> <li>○ systematic reporting (see paragraph 5.36);</li> <li>○ limiting or ceasing business (see paragraph 5.39).</li> </ul> |
|                      | 5.3 | The requirements to carry out CDD measures and ongoing monitoring build on the similar obligation under the ML Regulations. The requirements for systematic reporting and limiting or ceasing business are new.  |
|                      | 5.4 | Orders under POCA and Terrorism Act cannot be issued by HM Treasury; they are issued by judges in connection with law enforcement investigations into money laundering. Such orders are, therefore, very specific. It is possible that a direction by HM Treasury could impose requirements which overlap with the effect of an order under POCA or Terrorism Act although HM Treasury are working with SOCA to avoid this.  |

### *What grounds must HM Treasury have for issuing directions?*

- |                   |     |   |
|-------------------|-----|---|
| CTA Sch 7, para 1 | 5.5 | The Treasury may give a direction <b>if one or more</b> of the following conditions is met in relation to a non-EEA country: <ul style="list-style-type: none"> <li>○ that the Financial Action Task Force has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities being carried on             <ul style="list-style-type: none"> <li>(a) in the country,</li> <li>(b) by the government of the country, or</li> <li>(c) by persons resident or incorporated in the country.</li> </ul> </li> <li>○ that the Treasury reasonably believe that there is a risk that terrorist</li> </ul> |
|-------------------|-----|---|

financing or money laundering activities are being carried on

- (a) in the country,
- (b) by the government of the country, or
- (c) by persons resident or incorporated in the country,

**and** that this poses a significant risk to the national interests of the UK.

- o that the Treasury reasonably believe that
  - (a) the development or production of nuclear, radiological, biological or chemical weapons in the country, or
  - (b) the doing in the country of anything that facilitates the development or production of any such weapons,
 poses a significant risk to the national interests of the UK.

5.6 There are therefore a number of restrictions on the use of the powers by HM Treasury:

- o They can only be issued in relation to activities believed to be being carried on in a particular non-EEA jurisdiction;
- o Unless the FATF have advised that additional measures should be taken, HM Treasury must ‘reasonably believe’ that
  - o relevant activities (see paragraph 5.24) are being carried on **and**
  - o that this poses a significant risk to UK national interests.

Regulation 18

5.7 The restriction in relation to countries subject to advisory measures by FATF differs from the condition under which HM Treasury may exercise powers under the ML Regulations. The power under the Regulations is only exercisable in relation to countries in respect of which FATF have recommended counter measures, and is limited to directing a firm to cease entering into business relationships or carrying out occasional transactions with a person situated or incorporated in that country. The powers to issue directions under the CTA are broader, reflecting the range of counter measure options identified by the FATF.

CTA, Sch 7, para 2

5.8 Money laundering is defined in CTA Sch 7 by cross reference to s340(11) of POCA. Terrorist financing, however, is specifically defined in CTA Sch 7, but in different terms from that in the Terrorism Act.

5.9 HM Treasury are to issue specific guidance on the requirements of any directions made. These will be available on HM Treasury’s website [http://www.hm-treasury.gov.uk/fin\\_crime\\_policy.htm](http://www.hm-treasury.gov.uk/fin_crime_policy.htm).

*What firms may be subject to these directions?*

CTA, Sch 7, paras 3, 4

5.10 Directions under the CTA Sch 7 may only be given to persons (i.e., firms) operating in the financial sector. A person operating in the financial sector is defined as one that is a credit or financial institution

that is either a UK person or is acting in the course of a business carried on by it in the UK.

- CTA Sch 7, para 5(2)(g)  
Regulation 3(2),(3) 5.11 The definition of credit institution is the same as that in the ML Regulations, but the definition of financial institution contains an additional category of firm – an insurance company as defined by section 1165(3) of the Companies Act 2006. This extends the scope to include all insurance companies authorised under Part IV of FSMA, as well as Lloyd’s underwriters and companies offering vehicle accident or breakdown cover. However, firms brought into the scope of CTA Sch 7 only through this definition are only subject to two of the four categories of direction. Life assurance companies are therefore subject to all four categories of direction, as they are within the definition of financial institution in the ML Regulations.
- 5.12 These firms are excluded from the scope of the first two direction powers because those brought in are not currently required to carry out CDD measures or ongoing monitoring under the ML Regulations – in proposing the new powers, HM Treasury were seeking to be consistent with what firms were already required to do, and so had systems for. But the additional firms were included in the other two direction powers as these do not directly flow from the ML Regulations, and HM Treasury would expect all firms in the industry to have to implement them to address the potentially substantial risks against which they might be used.
- CTA Sch 7, para 3(1) 5.13 HM Treasury may issue directions to
- o A particular person operating in the financial sector; **or**
  - o Any description of persons in that sector; **or**
  - o All persons operating in that sector
- CTA Sch 7, para 14 5.14 Where directions are given to firms of a given type or to all firms, generally an Order must be laid before parliament by HM Treasury under the negative resolution procedure. The exception is a direction to limit or cease business, which requires an Order laid under the affirmative resolution procedure.
- SI 2009/2725 5.15 As an example, the first Order under CTA Sch 7 was laid on 12 October 2009. The order was in respect of two Iranian entities, Bank Mellat and Islamic Republic of Iran Shipping Lines, and was accompanied by an interpretive note issued by HM Treasury – the interpretive note is at [http://www.hm-treasury.gov.uk/d/fin\\_crime\\_interpretive\\_note.pdf](http://www.hm-treasury.gov.uk/d/fin_crime_interpretive_note.pdf).
- 5.16 Firms may obtain direct electronic notification of any such orders, interpretive notes and other HM Treasury-originated publications or announcements relating to the exercise of powers under CTA Sch 7 by subscribing to the HM Treasury AML/CTF mailing list – see [http://www.hm-treasury.gov.uk/fin\\_crime\\_mailinglist.htm](http://www.hm-treasury.gov.uk/fin_crime_mailinglist.htm).

*What directions may be imposed?*

- CTA Sch 7, para 9(1) 5.17 Requirements may be imposed in relation to transactions or business

- relationships with
- A person carrying on business in a particular country
  - The government of that country
  - A person resident or incorporated in that country
- CTA Sch 7, para 9(2) 5.18 A direction may impose requirements in relation to
- a particular person described in paragraph 5.17,
  - any description of persons detailed in that paragraph, or
  - all persons detailed in that paragraph.
- Any person in relation to whom a direction is given is a 'designated person' for the purposes of a direction.
- CTA Sch 7, para 9(4) 5.19 As mentioned in paragraph 5.2, the kinds of requirement that may be imposed by a direction relate to
- customer due diligence (see paragraphs 5.21ff);
  - ongoing monitoring (see paragraphs 5.31ff);
  - systematic reporting (see paragraphs 5.36ff);
  - limiting or ceasing business (see paragraphs 5.39ff).
- CTA Sch 7, para 15(3) 5.20 Any direction (if not previously revoked and whether or not varied) ceases to have effect after one year from the day it is given (although a further direction may be given).

*Customer due diligence*

- CTA Sch 7, para 10 5.21 The requirements in relation to customer due diligence that may be imposed relate to
- timing of carrying out enhanced due diligence
  - obligation to carry out enhanced due diligence
  - content of CDD measures
- Regulations 5, 7, 9  
Regulation 14 5.22 The general obligation to carry out CDD measures, and the timing and content of such measures, are already set out in the ML Regulations (although expressed in slightly different language from CTA Sch 7). EDD measures are also already required under the ML Regulations, but only in relation to the types of customer/product situation that are specified in the Regulation. Guidance on meeting the obligation to carry out EDD is given in Part I, section 5.5.
- 5.23 The specified requirements that may be imposed under a direction may differ in detail from the general requirements for CDD measures under the ML Regulations, although HM Treasury intend to direct similar requirements unless there are specific reasons to apply different requirements. As mentioned in paragraph 5.11, insurance companies (as defined there) may not be made subject to a direction under this paragraph of Schedule 7.

## Timing

- Regulation 7 (c)  
CTA Sch 7, para 10 (3),  
(4) 5.24 Under the ML Regulations a firm must carry out CDD measures when, inter alia, it suspects money laundering or terrorist financing. The powers under the CTA permit HM Treasury to direct that firms must carry out enhanced CDD of specified entities where it reasonably believes that there is a risk of money laundering or terrorist financing in a country, or that the development or production of nuclear, radiological, biological or chemical weapons, or the facilitation of such development or production in a country (the latter are collectively referred to as 'relevant activities'), poses a significant risk to the national interests of the UK.
- CTA Sch 7, para 10(1) 5.25 A direction may require a firm to undertake enhanced customer due diligence measures—
- (a) before entering into a transaction or business relationship with a designated person, and
  - (b) during a business relationship with such a person.
- 5.26 In practical terms, if such requirements are imposed under a direction from HM Treasury, a firm would not be expected to apply CDD measures at a point that was different from that in respect of which guidance is given in Part I, section 5.2, unless specifically directed to (although the exceptions referred to in paragraphs 5.2.3 - 5.2.5 would not apply, as the firm would be under a specific direction, thus indicating a high risk of money laundering or terrorist financing that requires checks before any access to the financial system is facilitated).

## Enhanced due diligence

- CTA Sch 7, para 10(2) 5.27 The direction may
- (a) impose a general obligation to undertake enhanced customer due diligence measures; and/or
  - (b) require a firm to undertake specific measures identified or described in the direction.
- 5.28 In practical terms, if such requirements are imposed under a direction from HM Treasury, a firm would not be expected to apply different EDD measures from those carried out in accordance with the guidance given in Part I, section 5.5, unless specifically directed to. The discretion in the risk-assessment as to whether EDD should be applied is removed through a direction having been given; within this, however, there will still be discretion to determine the extent of EDD measures appropriate in each case (unless these are specified in the direction).

## Content of CDD measures

- CTA Sch 7, para 10(3) 5.29 “Customer due diligence measures” is defined in CTA Sch 7 as measures
- (a) to establish the identity of the designated person (see paragraph 5.18),
  - (b) to obtain information about—
    - (i) the designated person and their business, and
    - (ii) the source of their funds, and
  - (c) to assess the risk of the designated person being involved in relevant activities.
- 5.30 In practical terms, if such requirements are imposed under a direction from HM Treasury, a firm would not be expected to apply different CDD measures from those carried out in accordance with the guidance given in Part I, section 5.3, unless specifically directed to.

*Ongoing monitoring*

- CTA Sch 7, para 11(1), (2) 5.31 A direction may require a firm to undertake enhanced ongoing monitoring of any business relationship with a designated person. The direction may
- (a) impose a general obligation to undertake enhanced ongoing monitoring; and/or
  - (b) require a firm to undertake specific measures identified or described in the direction.
- Regulation 8  
Regulation 14 (1), (4)(c) 5.32 The general obligation to carry out ongoing monitoring is already set out in the ML Regulations (although expressed in slightly different language from CTA Sch 7). Enhanced ongoing monitoring is required generally in relation to higher risk situations, and specifically where the customer is a PEP. Guidance on carrying out ongoing monitoring is set out in Part I, section 5.7.
- 5.33 As mentioned in paragraph 5.11, insurance companies (as defined there) may not be made subject to a direction under this paragraph of Schedule 7.
- CTA Sch 7, para 11(3) 5.34 “Ongoing monitoring” of a business relationship is defined in CTA Sch 7 as
- (a) keeping up to date information and documents obtained for the purposes of customer due diligence measures, and
  - (b) scrutinising transactions undertaken during the course of the relationship (and, where appropriate, the source of funds for those transactions) to ascertain whether the transactions are consistent with the firm’s knowledge of the designated person and their business.
- 5.35 In practical terms, if such requirements are imposed under a direction from HM Treasury, a firm would not be expected to apply different enhanced ongoing monitoring from that carried out in accordance with

the guidance given in Part I, section 5.7, unless specifically directed to.

*Systematic reporting*

- |                       |      |  |
|-----------------------|------|--|
| CTA Sch 7, para 12(1) | 5.36 | A direction may require a firm to provide such information and documents as may be specified in the direction relating to transactions and business relationships with designated persons.   |
| CTA Sch 7, para 12(2) | 5.37 | A direction imposing such a requirement must specify how the direction is to be complied with, including <ul style="list-style-type: none"> <li>(a) the person to whom the information and documents are to be provided, and</li> <li>(b) the period within which, or intervals at which, information and documents are to be provided.</li> </ul> |
|                       | 5.38 | Transactions that are subject to a direction imposing systematic reporting are very likely to be prospective. Although it is possible that historic data may be requested, this would likely only result from a follow up to a previous systematic reporting order.  |

*Limiting or ceasing business*

- |                                |      |  |
|--------------------------------|------|--|
| CTA Sch 7, para 13             | 5.39 | A direction may require a firm not to enter into or continue to participate in <ul style="list-style-type: none"> <li>(a) a specified transaction or business relationship with a designated person, or</li> <li>(b) a specified description of transactions or business relationships with a designated person, or</li> <li>(c) any transaction or business relationship with a designated person.</li> </ul> |
| Regulation 18                  | 5.40 | This power is broader than the power in the ML Regulations given to HM Treasury in relation to customers from non-EEA states to which the FATF have decided to apply counter measures.   |
|                                | 5.41 | The obligation to limit or cease business with a designated person is different from the obligation not to do business with a name on a sanctions list. The CTA direction is more flexible, and can be applied more broadly; it also does not involve freezing a customer's assets.  |
|                                | 5.42 | There may be situations where a firm itself prefers to close a relationship with a designated person. In such circumstances it might be important to consult with HM Treasury before taking that action.   |
| CTA Sch 7, para 17 (1)–<br>(4) | 5.43 | HM Treasury may grant a licence to exempt acts specified in the licence  |

from requirements in a direction to limit or cease business. A licence may be

- (a) general or granted to a description of persons or to a particular person;
- (b) subject to conditions;
- (c) of indefinite duration or subject to an expiry date.

HM Treasury may vary or revoke a licence at any time.

- CTA Sch 7, para 17 (5) 5.44 On the grant, variation or revocation of a licence, HM Treasury must
- (a) in the case of a licence granted to a particular person, give notice of the grant, variation or revocation to that person;
  - (b) in the case of a general licence or a licence granted to a description of persons, take such steps as HM Treasury consider appropriate to publicise the grant, variation or revocation of the licence.

*Enforcement and penalties for non-compliance*

- CTA Sch 7, paras 25, 30 5.45 A firm may be penalized for a failure to comply with a requirement under a direction in one of two ways:
- A civil penalty by the supervisory and enforcement authority (the FSA); or
  - Criminal prosecution for the failure

- CTA Sch 7, para 25(5), 30(6) 5.46 A firm cannot be made liable to a civil penalty and be prosecuted for the same failure.

- CTA Sch 7, para 25(3), 30(3) 5.47 In deciding whether to impose a penalty, or whether a firm has committed an offence, in relation to a failure to comply with a requirement, an enforcement authority or a court must consider whether the firm followed any relevant guidance which was at the time
- (a) issued by a supervisory authority or any other appropriate body,
  - (b) approved by the Treasury, and
  - (c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it.

*Civil penalty*

- CTA Sch 7, para 25(1) 5.48 An enforcement authority may impose a penalty of such amount as it considers appropriate on a person who fails to comply with a requirement imposed
- (a) by a direction under Sch 7, or
  - (b) by a condition of a licence under such a direction.

- CTA Sch 7, para 25(2) 5.49 No such penalty is to be imposed if the authority is satisfied that the

person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with.

SYSC 6.1.1 R            5.50    Firms should note that the regulatory requirement to have in place adequate policies and procedures for countering the risk that a firm might be used to further financial crime - which includes terrorist financing - also applies. This means that the FSA can take regulatory action against a firm relating to its systems and controls, even where no breach of a direction under Schedule 7 of the CTA has occurred.

*Offence: failure to comply with requirement imposed by a direction*

CTA Sch 7, paras 30(1), 32(1)	5.51	Where a firm fails to comply with a requirement imposed by a direction under CTA Sch 7 it is open to criminal prosecution, subject to paragraph 5.51. An offence may be committed by a UK person by conduct wholly or partly outside the UK.
CTA Sch 7, para 30(2),	5.52	No offence is committed if the person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with.
CTA Sch 7, para 30(5)	5.53	The criminal sanction under CTA Sch 7 is a prison term of up to two years, and/or a fine.